RATIONALE for

CSPP - COTS Security Protection Profile - Operating Systems

(formerly: CS2-OS - Protection Profile for near-term COTS Operating Systems)

DRAFT VERSION 0.3

by Gary Stoneburner (NIST)

Date - 4/4/00

Revision History

Version 0.3, date 12/9/99, name change to reflect CS2 to CSPP change, incorporate editorial changes made in released version of CSPP, and deletion of requirement for trusted path with modification to related objective (not a part of most COTS OSs).

Version 0.2, date 7/27/99, editorial changes, completed TBDs in functional components, and added functional requirements for IT-environment.

Version 0.1, initial version, 3/25/99 - some TBDs (operations on functional components and functional requirements details for the IT-environment).

DRAFT, SUBJECT to CHANGE

NIST United States Department of Commerce
National Institute of Standards and Technology

DRAFT

TABLE OF CONTENTS

SECTION **PAGE**

TABLE OF TABLES

TABLE **PAGE**

1.0 INTRODUCTION

The purpose of this rationale document is to show that the CSPP-OS protection profile (PP) is internally consistent, accurate, and complete to a level of confidence corresponding to the EAL2 assurance level. This is accomplished by the individual rationales listed in Table 1-1.

Taken together, these rationale show (at a level of rigor appropriate for EAL-2 level evaluations) that the PP's list of functional and assurance requirements are suitable for describing a specific user need within the scope of those described in the CSPP-OS introduction and TOE description.

Table 1-1 CSPP-OS Rationale Overview

Nature of Rationale	Purpose	Section
Discuss the usage assumptions, showing that they are necessary and reasonable.	Show that the security environment description is consistent with the introduction and the TOE description.	2.1
Discuss the security policies, showing that they are necessary and reasonable.		2.2
Discuss the security threats, showing that they are necessary and reasonable.		2.3
Discuss the general assurance level, showing that it is appropriate.		2.4
Map security objectives to policy and threat	Show necessity of CSPP-OS objectives	3.1
Map policy/threat to security objectives	Show completeness of CSPP-OS objectives	3.2
Compare environmental security objectives with CSPP-OS introduction and TOE description	Show correctness of CSPP-OS objectives	3.3
Map TOE functional requirement to dependencies and security objectives	Show necessity of CSPP-OS TOE functionality	4.1
Map TOE security objectives to TOE functional requirements and justify SOF claims	Show sufficiency of CSPP-OS TOE functionality	4.2
Map dependencies for CSPP-OS TOE functionality to CSPP-OS requirement meeting that dependency	Show correctness of CSPP-OS TOE functionality	4.3.1
Discuss operations performed on CSPP-OS TOE function components (iteration, assignment, selection, or refinement)		4.3.2
Discuss functional operations deferred to ST		4.3.3
Discuss non-CC functional extensions		4.3.4

Nature of Rationale	**Purpose**	**Section**
Discuss basic assurance goals	Show necessity of CSPP-OS assurances	5.1.1
Show EAL2 is the correct base level by mapping necessary components not in EAL2 to need and unnecessary components in EAL3 to rationale for being not needed.		5.1.2
Map EAL2 augmentation to need		5.1.3
Map unused CC components to reason for not being used	Show sufficiency of CSPP-OS assurances	5.2
Map dependencies for CSPP-OS assurance to CSPP-OS requirement meeting that dependency	Show correctness of CSPP-OS assurances	5.3.1
Discuss operations performed on CSPP-OS assurance components (iteration, assignment, selection, or refinement)		5.3.2
Discuss assurance operations deferred to ST		5.3.3
Discuss non-CC assurance extensions		5.3.4

2.0 SECURITY ENVIRONMENT RATIONALE

2.1 USAGE ASSUMPTIONS

This rationale shows that each of the CSPP-OS usage assumptions is necessary and reasonable in light of the CSPP-OS introduction and TOE description. This is accomplished in Table 2.1-1.

Table 2.1-1 Usage Assumption Rationale

Name	Assumption	Rationale
A. ADMIN	The security features of the TOE are competently administered on an on-going basis.	This is widely recognized, even if system administration is not always afforded the importance it deserves. Unless the system is administered competently in an on-going manner, security is not feasible. Therefore this assumption is both necessary and reasonable.
A.COTS	The TOE is constructed from near-term achievable, commercial off the shelf information technology.	This assumption is a stated part of the design criteria for this PP and is a key driver in determining the nature of the expectations toward, and hence the requirements to placed upon, the TOE. Therefore this assumption is both necessary and reasonable.
A.MALICIOUS-INSIDER	The TOE is not expected to be able to sufficiently mitigate the risks resulting from malicious abuse of authorized privileges.	It is important to explicitly recognize that it is not reasonable to expect near-term COTS products to provide sufficient protection against the malicious actions of authorized individuals. Therefore this assumption is both necessary and reasonable.
A.NO-LABELS	The TOE does not have to provide label-based access controls.	This assumption is used in the production of this PP and it is considered important to state this explicitly. Therefore this assumption is both necessary and reasonable.
A.SOPHISTICATED-ATTACK	The TOE is not expected to be able to sufficiently mitigate risks resulting from application of sophisticated attack methods.	It is important to explicitly recognize that it is not reasonable to expect near-term achievable COTS to be able to resist sophisticated attacks. Therefore this assumption is both necessary and reasonable.
A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	Unless the users internalize a need for security they are bound to circumvent it. This fact is commonly recognized and a primary driver in security awareness training that is common place both in government and industry. Therefore this assumption is both necessary and reasonable.

Name	Assumption	Rationale
A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	The authenticated users are trusted in this manner in most organizations. With CSPP-OS compliant TOEs, the users have a fair amount of discretion and must be trusted to handle it appropriately. Therefore this assumption is both necessary and reasonable.

2.2 SECURITY POLICIES

Table 2.2-1 presents the rationale showing that each of the CSPP-OS security policies is both necessary and reasonable.

Table 2.2-1 Security Policy Rationale

Name	Policy	Rationale
P.ACCESS	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.	It is an essential premise for CSPP-OS TOEs that the access to objects is controlled. The nature of this control is clearly that characteristics of the proposed access (entity, type of access; e.g., read, write, and nature of access; e.g., local, remote, time-of-day) are compared with attributes of the object to determine whether the access to be allowed. This policy is both necessary and reasonable.
P.ACCOUNT	Users must be held accountable for security-relevant actions.	It is generally considered standard, best practice to hold users accountable for their actions. This policy is necessary and reasonable.
P.COMPLY	The implementation and use of the organization's IT must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	This policy is necessary and reasonable.
P.DUE-CARE	The organization's IT systems must be implemented and operated in a manner the represents due care and diligence with respect to risks to the organization.	As IT becomes a central part of the business or mission process, the potential impact on the organization, and personally on the organization's senior management, has dramatically increased. With this is coming the recognition that due care and diligence with respect to computing security is now as important as the organization's fiduciary responsibilities in other areas. The policy is necessary and reasonable.
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	Most organizations will have a mandatory information flow control policy to deal with information such as company proprietary data and information under contractual or statutory limitations. So, in the general case, this policy is necessary and reasonable.
P.KNOWN	Except for a well-defined set of allowed operations, users of the TOE must be identified and authenticated before TOE access can be granted.	It is standard practice to identify and authenticate users. It has also become common to allow anonymous access in cases such as a public web server. This policy is necessary and reasonable.

Name	Policy	Rationale
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	Distributed information systems is a fact that CSPP-OS must incorporate. This policy is necessary and reasonable.
P.PHYSICAL	The processing resources of the TOE that must be physically protected in order to ensure that security objectives are met will be located within controlled access facilities that mitigate unauthorized, physical access.	It is commonly recognized that the TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided. Providing such protection is a common element of organizational policies. This policy is necessary and reasonable.
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	Since IT has become an essential component of many mission/business processes, this is a key element of a successful computing security program. This is also becoming widely understood as such. This policy is necessary and reasonable.
P.TRAINING	Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	Organizations generally accept this as a need and are implementing it. Unless the users are able to make appropriate choices, they are likely to defeat the security controls. This policy is necessary and reasonable.
P.USAGE	The organization's IT resources must be used for only for authorized purposes.	While "use for only authorized purposes" has been a common policy for some time, this policy is even more important with recent hacking to use corporate and government resources for a number of unauthorized activities like spamming, software piracy, and breaking other systems. This policy is necessary and reasonable.

2.3 THREATS TO SECURITY

For each threat addressed by this PP, Table 2.3-1 gives a rationale for that threat, explaining why, if not met by the TOE, it is appropriate to be classed as environment or joint.

Table 2.3-1 Security Threat Rationale

Name	Threat	Rationale
Environment: T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.	Like T-ENTRY-NON-TECHNICAL, this threat is explicitly non-technical and its mitigation requires environmental controls. T.ACCESS-NON-TECHNICAL is listed as a separate threat from T.ENTRY-NON-TECHNICAL because the likely mitigating controls applied to authenticated users are different from those applied to individuals not authorized IT access.
Environment: T.ACCESS-Non-TOE	An authenticated user may gain unauthorized, non-malicious access to a resource or to information not directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.	The TOE cannot, in general, be expected to protect other components of the system from such attacks. Therefore, mechanisms within these other components must provide this protection.
Environment: T.AUDIT-CONFIDENTIALITY-Non-TOE	For audit trails not under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	For audit records not under control of the TOE, other components within the system must address this threat.
Environment: T.AUDIT-CORRUPTED-Non-TOE	For audit trails not under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	For audit records not under control of the TOE, other components within the system must address this threat.
Environment: T.DENIAL-Non-TOE	The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.	The TOE cannot, in general, be expected to protect other components of the system from such attacks. Therefore, mechanisms within these other components must provide this protection.
Environment: T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.	The TOE is not capable of resisting sophisticated attacks and must therefore, rely on protections provided by its environment to maintain availability in the face of such threats.
Environment: T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.	This threat is explicitly non-technical and beyond the scope of CSPP technical controls. This necessitates environmental controls.

Name	Threat	Rationale
Environment: T.ENTRY-Non-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.	The TOE cannot, in general, be expected to protect other components of the system from such attacks. Therefore, mechanisms within these other components must provide this protection.
Environment: T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.	The TOE is not expected to be able to protect against sophisticated, technical attacks. There is no reasonable expectation that a TOE compliant with a CSPP-OS PP will significantly increase, over that associated with a non-compliant TOE, the work-factor required to accomplish a successful, high-grade attack. Therefore, this threat is largely addressed by the TOE environment.
Environment: T.OBSERVE-Non-TOE	Events occur in operation of IT (other than the TOE) that compromise IT security; but that IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.	The TOE cannot, in general, be expected to protect other components of the system from such attacks. Therefore, mechanisms within these other components must provide this protection.
Environment: T.PHYSICAL	Security-critical parts of the TOE may be subjected to a physical attack that may compromise security.	As explained in the discussion concerning P.PHYSICAL the physical protection of IT resources is critical. Since CSPP-OS is a baseline for near-term COTS, it is not reasonable to expect TOE mechanisms that address physical security to any significant degree.
Environment: T.RECORD-EVENT-Non-TOE	Security relevant events not under control of the TOE may not be recorded.	For auditing not under control of the TOE, other components within the system must address this threat.
Environment: T.TRACEABLE-Non-TOE	Security relevant events not under control of the TOE may not be traceable to the user or system process associated with the event.	For auditing not under control of the TOE, other components within the system must address this threat.
Joint: T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.	The TOE mechanisms for controlling access will help address this threat. But since CSPP is a baseline for near-term COTS, this mitigation is not likely to be sufficient for the risks implied by this threat. Hence additional, environmental controls are essential. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.

Name	Threat	Rationale
Joint: T.ADMIN-ERROR	The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.	Humans make mistakes, and if that human is the system administrator then the security consequences may be great. The TOE is expected to provide some mitigation, but, especially since CSPP is a baseline for near-term COTS, the TOE controls are not expected to be adequate. Environmental controls are needed as well. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.
Joint: T.CRASH-SYSTEM	The secure state of the system could be compromised in the event of a system crash.	As an underlying operating system, the TOE is expected to cooperate with its environment in addressing this threat. However, as only one component of the system, the TOE is unable (in general) to ensure recovery for IT other than itself.
Joint: T.INSTALL	The TOE may be delivered or installed in a manner that undermines security.	The TOE can be expected to help address this threat, but significant environmental controls are also expected. There is the distinct potential for trade-offs between environment and TOE in meeting this threat, while maintaining consistency with the intent and constraints of this PP.
Joint: T.OPERATE	Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.	While the TOE can be expected to provide mechanisms that help cover this threat, full coverage inherently includes actions that must be addressed by environmental controls. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.
Joint: T.SYSTEM-CORRUPTED	The security state of the TOE, as a result of another threat, may be intentionally corrupted to enable future insecurities.	System penetrations by either sophisticated attackers or attackers using sophisticated tools will likely result in an intentionally corrupted system state. A CSPP-OS compliant TOE is not expected to adequately mitigate against such a corruption. The TOE mechanisms are expected, in concert with environmental controls, to support detection of such corruption. A compliant solution may provide for some trade-off between environment and TOE in meeting this threat.

Name	Threat	Rationale
TOE: T.ACCESS-TOE	An authenticated user may gain unauthorized, non-malicious access to the TOE, or a resource or to information directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.	Users are generally trusted to do the right thing (A.USER-TRUST). However, they will make mistakes and it is likely that situations will occur where users circumvent security "to get the job done", out of curiosity, or for the sake of the challenge to do so. CSPP-OS technical controls are limited to addressing this threat, in lieu of the threat of malicious user actions, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from malicious actions is beyond the scope of CSPP expectations.
TOE: T.AUDIT-CONFIDENTIALITY-TOE	For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CONFIDENTIALITY-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability.
TOE: T.AUDIT-CORRUPTED-TOE	For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.AUDIT-CORRUPTED-TOE is highlighted as a contributor toward a potential failure in the detection and response capability.
TOE: T.CRASH-TOE	The secure state of the TOE could be compromised in the event of a system crash.	Systems crash and secure systems may crash into an insecure state. Mitigating against this is reasonable, prudent, and within the scope of CSPP technical controls.
TOE: T.DENIAL-TOE	The TOE may be subjected to an unsophisticated, denial-of-service attack.	In the real-world, CSPP systems will be subjected to denial of service. This fact and the need to meet P.SURVIVE require addressing this threat. CSPP technical controls are limited to addressing this threat, in lieu of the threat of sophisticated attacks, because CSPP is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of CSPP expectations.
TOE: T.ENTRY-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to TOE controlled processing resources or information via an unsophisticated, technical attack.	CSPP-OS technical controls are limited to addressing this threat, in lieu of the threat of sophisticated attacks, because CSPP-OS is a baseline for COTS that is near-term achievable. Protecting against the greater risk from sophisticated actions is beyond the scope of CSPP expectations.

Name	Threat	Rationale
TOE: T.OBSERVE-TOE	Events occur in TOE operation that compromise IT security but the TOE, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.	CSPP systems must not misrepresent what is within the scope of their security mechanisms to correctly interpret. The man-machine interface, at least with respect to the basic security state of the system, must be free from obvious errors that might lead an responsible, competent individual to misunderstand the system's security state.
TOE: T.RECORD-EVENT-TOE	Security relevant events controlled by the TOE may not be recorded.	Because CSPP is not intended to be able to resist all attacks, detection and response are critical. T.RECORD-EVENT-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability.
TOE: T.RESOURCES	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.	CSPP-OS represents, in general, multi-user or multi-process systems. As such, mechanisms addressing this threat are common place and typically a part of the OS rather than other IT elements of the system.
TOE: T.TOE-CORRUPTED	The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.	For these lower-grade attacks, the TOE is expected to provide the mechanisms necessary to address purposeful corruption in support of producing future insecurities.
TOE: T.TRACEABLE-TOE	Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.	Because CSPP-OS is not intended to be able to resist all attacks, detection and response are critical. T.TRACEABLE-TOE is highlighted as a significant contributor toward a potential failure in the detection and response capability.

2.4 GENERAL ASSURANCE LEVEL

The rationale for the general level of assurance for CSPP-OS is fully covered in sections 5.1.1 "Basic Assurance Goals" and 5.1.2 "EAL Selection".

3.0 SECURITY OBJECTIVES RATIONALE

The rationale for the set of CSPP security objectives will be based upon the following:

- Necessity – all required. Each objective must contribute to satisfying a security policy or countering a threat.
- Complete – satisfy all policies and counter all threats. The list of security objectives must satisfy the policies and adequately counter the threats listed in CSPP.
- Correct –
  - TOE verses environment. The allocation of policy enforcement and threat mitigation to the environment must be reasonable.
  - Correct statement. The security objective must correctly state its intent.

3.1 NECESSARY OBJECTIVES

Table 3.1-1 shows the mapping of security objectives to threats and policies. This table indicates that each objective contributes to countering a threat or satisfying a policy. Thus there are no unnecessary objectives.

Table 3.1-1 Necessary Objectives – Mapping Objectives to Policy and Threat

Security Objective	Threats (T.*) and Policies (P.*)
O.ACCESS-MALICIOUS: The TOE controls will help in achieving this objective, but will not be sufficient. Additional, environmental controls are required to sufficiently mitigate the threat of malicious actions by authenticated users. This will be accomplished by focusing on deterrence, detection, and response with a goal of moderate effectiveness.	T.ACCESS-MALICIOUS
O.ACCESS-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by authenticated users for non-malicious purposes. This will be accomplished primarily via prevention with a goal of high effectiveness. Personnel security and user training and awareness will provide a major part of achieving this objective.	T.ACCESS-NON-TECHNICAL
O.ACCESS-Non-TOE: The IT other than the TOE must provide public access and access by authenticated users to the resources and actions for which they have been authorized and over which the TOE does not exercise control. The focus is on prevention with a high degree of effectiveness.	P.ACCESS
O.ACCESS-TOE: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized. This will be accomplished with high effectiveness.	P.ACCESS
O.ACCOUNT-Non-TOE: The IT other than the TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions. This is expected with a high degree of effectiveness.	P.ACCOUNT T.TRACEABLE-Non-TOE T.RECORD-EVENT-Non-TOE T.AUDIT-CORRUPTED-Non-TOE T.AUDIT-CONFIDENTIALITY-Non-TOE

Security Objective	Threats (T.*) and Policies (P.*)
O.ACCOUNT-TOE: The TOE must ensure, for actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions. This will be done with moderate effectiveness, in that it is anticipated that individual accountability might not be achieved for some actions.	P.ACCOUNT T.TRACEABLE-TOE T.RECORD-EVENT-TOE T.AUDIT-CORRUPTED-TOE T.AUDIT-CONFIDENTIALITY-TOE
O.AUTHORIZE-Non-TOE: The IT other than the TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This is expected with a high degree of effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS
O.AUTHORIZE-TOE: The TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This will be accomplished with high effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS
O.AVAILABLE-Non-TOE: The IT other than the TOE must protect itself from unsophisticated, denial-of-service attacks. This is a combination of prevention and detect and recover with a high degree of effectiveness.	P.SURVIVE T.DENIAL-Non-TOE
O.AVAILABLE-TOE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection with high effectiveness.	P.SURVIVE T.DENIAL-TOE
O.BYPASS-Non-TOE: For access not controlled by the TOE, IT other than the TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because IT controls in the notional CSPP system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS-Non-TOE

Security Objective	Threats (T.*) and Policies (P.*)
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to ‘non-malicious’ because CSPP-OS controls are not expected to be sufficient mitigation for the greater negative impact that ‘malicious’ implies.	T.ACCESS-TOE
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements. This will be accomplished via some technical controls, yet with a focus on non-technical controls to achieve this objective with high effectiveness.	P.COMPLY
O.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks. The focus is on detection and response with a goal of moderate effectiveness.	P.SURVIVE T.DENIAL-SOPHISTICATED
O.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state). The goal is for moderate effectiveness.	P.SURVIVE T.SYSTEM-CORRUPTED
O.DETECT-SYSTEM: The TOE, in conjunction with other IT in the system, must enable the detection of system insecurities. The goal is high effectiveness for lower grade attacks.	P.SURVIVE T.SYSTEM-CORRUPTED
O.DETECT-TOE: The TOE must enable the detection of TOE specific insecurities. The goal is high effectiveness for lower grade attacks.	P.SURVIVE T.TOE-CORRUPTED
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization. This will be accomplished via a combination of technical and non-technical controls to achieve this objective with high effectiveness.	P.DUE-CARE
O.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users. This will be accomplished primarily via prevention with a goal of high effectiveness. User training and awareness will provide a major part of achieving this objective.	T.ENTRY-NON-TECHNICAL
O.ENTRY-Non-TOE: For resources not controlled by the TOE, IT other than the TOE must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access. This is clearly a prevent focus and is to be achieved with a high degree of effectiveness.	P.USAGE T.ENTRY-Non-TOE
O.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack. This will be accomplished by focusing on detection and response with a goal of moderate effectiveness.	T.ENTRY-SOPHISTICATED

Security Objective	Threats (T.*) and Policies (P.*)
O.ENTRY-TOE: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access. This will be accomplished with high effectiveness.	P.USAGE T.ENTRY-TOE
O.INFO-FLOW: The TOE environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces. This will be accomplished by preventing unauthorized flows with high effectiveness.	P.INFO-FLOW
O.KNOWN-Non-TOE: The IT other than the TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This is expected with a high degree of effectiveness.	P.KNOWN
O.KNOWN-TOE: The TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This will be accomplished with high effectiveness.	P.KNOWN
O.MANAGE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security. This will be accomplished with moderate effectiveness.	T.ADMIN-ERROR
O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness.	P.NETWORK
O.OBSERVE-Non-TOE: The IT other than the TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-Non-TOE
O.OBSERVE-TOE: The TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	T.OBSERVE-TOE
O.OPERATE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that the system is delivered, installed, and operated in a manner which maintains IT security. This will be accomplished with moderate effectiveness.	T.INSTALL T.OPERATE P.TRAINING
O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security. This will be accomplished primarily via prevention with a goal of high effectiveness.	P.PHYSICAL T.PHYSICAL
O.RECOVER-SYSTEM: The system must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with some prevention and a majority of detect and respond, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	P.SURVIVE T.CRASH-SYSTEM

Security Objective	Threats (T.*) and Policies (P.*)
O.RECOVER-TOE: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with a high effectiveness for specified failures and a low effectiveness for failures in general.	P.SURVIVE T.CRASH-TOE
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	P.SURVIVE T.RESOURCES

3.2 COMPLETE OBJECTIVES

Table 3.2-1 shows that all policies and threats have related security objectives. While this alone does not prove completeness, a simple mapping is considered sufficient in light of the general level of assurance provided by EAL2.

Table 3.2-1 Complete Objectives – Mapping Policy and Threat to Objectives

Name	Description	Objectives
P.ACCESS	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.	O.ACCESS-NON-TECHNICAL O.ACCESS-NON-TOE O.AUTHORIZE-NON-TOE O.AUTHORIZE-TOE
P.ACCOUNT	Users must be held accountable for security-relevant actions.	O.ACCOUNT-NON-TOE O.ACCOUNT-TOE
P.COMPLY	The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	O.COMPLY
P.DUE-CARE	The organization's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to risks to the organization.	O.DUE-CARE
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	O.INFO-FLOW
P.KNOWN	Except for a well-defined set of allowed operations, users of the TOE must be identified and authenticated before TOE access can be granted.	O.KNOWN-NON-TOE O.KNOWN-TOE
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	O.NETWORK

Name	**Description**	**Objectives**
P.PHYSICAL	The processing resources of the TOE that must be physically protected in order to ensure that security objectives are met will be located within controlled access facilities that mitigate unauthorized, physical access.	O.PHYSICAL
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	O.AVAILABLE-NON-TOE O.AVAILABLE-TOE O.DENIAL-SOPHISTICATED O.DETECT-SOPHISTICATED O.DETECT-SYSTEM O.DETECT-TOE O.RECOVER-SYSTEM O.RECOVER-TOE O.RESOURCES
P.TRAINING	Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	O.OPERATE
P.USAGE	The organization's IT resources must be used for only for authorized purposes.	O.ENTRY-NON-TOE O.ENTRY-TOE
T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.	O.ACCESS-MALICIOUS
T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.	O.ACCESS-NON-TECHNICAL
T.ACCESS-Non-TOE	An authenticated user may gain unauthorized, non-malicious access to a resource or to information not directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.	O.BYPASS-NON-TOE

Name	**Description**	**Objectives**
T.ACCESS-TOE	An authenticated user may gain unauthorized, non-malicious access to the TOE, or a resource or to information directly controlled by the TOE via user error, system error, or an unsophisticated, technical attack.	O.BYPASS-TOE
T.ADMIN-ERROR	The security of the system may be reduced or defeated due to errors or omissions in the administration of the security features of the system.	O.MANAGE
T.AUDIT-CONFIDENTIALITY-Non-TOE	For audit trails not under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	O.ACCOUNT-NON-TOE
T.AUDIT-CONFIDENTIALITY-TOE	For audit trails under control of the TOE, records of security events may be disclosed to unauthorized individuals or processes.	O.ACCOUNT-TOE
T.AUDIT-CORRUPTED-Non-TOE	For audit trails not under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	O.ACCOUNT-NON-TOE
T.AUDIT-CORRUPTED-TOE	For audit trails under control of the TOE, records of security events may be subjected to unauthorized modification or destruction.	O.ACCOUNT-TOE
T.CRASH-SYSTEM	The secure state of the system could be compromised in the event of a system crash.	O.RECOVER-SYSTEM
T.CRASH-TOE	The secure state of the TOE could be compromised in the event of a system crash.	O.RECOVER-TOE
T.DENIAL-Non-TOE	The IT (other than the TOE) may be subjected to an unsophisticated, denial-of-service attack.	O.AVAILABLE-NON-TOE
T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.	O.DENIAL-SOPHISTICATED
T.DENIAL-TOE	The TOE may be subjected to an unsophisticated, denial-of-service attack.	O.AVAILABLE-TOE

Name	**Description**	**Objectives**
T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.	O.ENTRY-NON-TECHNICAL
T.ENTRY-Non-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information not controlled by the TOE via an unsophisticated, technical attack.	O.ENTRY-NON-TOE
T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.	O.ENTRY-SOPHISTICATED
T.ENTRY-TOE	An individual other than an authenticated user may gain unauthorized, malicious access to TOE controlled processing resources or information via an unsophisticated, technical attack.	O.ENTRY-TOE
T.INSTALL	The system may be delivered or installed in a manner that undermines security.	O.OPERATE
T.OBSERVE-Non-TOE	Events occur in operation of IT (other than the TOE) that compromise IT security; but that IT, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.	O.OBSERVE-NON-TOE
T.OBSERVE-TOE	Events occur in TOE operation that compromise IT security but the TOE, due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.	O.OBSERVE-TOE
T.OPERATE	Security failures may occur because of improper operation of the system; e.g., the abuse of authorized privileges.	O.OPERATE

Name	**Description**	**Objectives**
T.PHYSICAL	Security-critical parts of the system may be subjected to a physical attack that may compromise security.	O.PHYSICAL
T.RECORD-EVENT-Non-TOE	Security relevant events not under control of the TOE may not be recorded.	O.ACCOUNT-NON-TOE
T.RECORD-EVENT-TOE	Security relevant events controlled by the TOE may not be recorded.	O.ACCOUNT-TOE
T.RESOURCES	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.	O.RESOURCES
T.SYSTEM-CORRUPTED	The security state of the system, as a result of another threat, may be intentionally corrupted to enable future insecurities.	O.DETECT-SOPHISTICATED O.DETECT-SYSTEM
T.TOE-CORRUPTED	The security state of the TOE, as a result of a lower-grade attack, may be intentionally corrupted to enable future insecurities.	O.DETECT-TOE
T.TRACEABLE-Non-TOE	Security relevant events not under control of the TOE may not be traceable to the user or system process associated with the event.	O.ACCOUNT-NON-TOE
T.TRACEABLE-TOE	Security relevant events controlled by the TOE may not be traceable to the user or system process associated with the event.	O.ACCOUNT-TOE

3.3 CORRECT OBJECTIVES

Table 3.3-1 provides a rationale for the correctness of each of security objectives. Where there is a one-to-one match between a policy or threat, that policy or threat is the rationale. For the environmental and joint objectives, an explanation is provided for not including the objective in the list of TOE security objectives.

Table 3.3-1 Correct Objectives - Mapping Security Objective to Rationale

Security Objective	Type	Rationale
O.ACCESS-MALICIOUS: The TOE controls will help in achieving this objective, but will not be sufficient. Additional, environmental controls are required to sufficiently mitigate the threat of malicious actions by authenticated users. This will be accomplished by focusing on deterrence, detection, and response with a goal of moderate effectiveness.	Joint	T.ACCESS-MALICIOUS As the underlying OS, the TOE is expected to provide support for this objective. Since the OS is a baseline at EAL2, the TOE is not expected to be able to meet this objective and extensive support from its environment will be needed. Hence this is joint.
O.ACCESS-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by authenticated users for non-malicious purposes. This will be accomplished primarily via prevention with a goal of high effectiveness. Personnel security and user training and awareness will provide a major part of achieving this objective.	Env	T.ACCESS-NON-TECHNIAL The nature of this threat precludes its being addressed by TOE mechanisms. Hence this is environmental.
O.ACCESS-Non-TOE: The IT other than the TOE must provide public access and access by authenticated users to the resources and actions for which they have been authorized and over which the TOE does not exercise control. The focus is on prevention with a high degree of effectiveness.	Env	T.ACCESS-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.
O.ACCESS-TOE: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized. This will be accomplished with high effectiveness.	TOE	T.ACCESS-TOE
O.ACCOUNT-Non-TOE: The IT other than the TOE must ensure, for actions under its control or knowledge, that all users can subsequently be held accountable for their security relevant actions. This is expected with a high degree of effectiveness.	Env	P.ACCOUNT T.TRACEABLE-NON-TOE T.RECORD-EVENT-NON-TOE T.AUDIT-CORRUPTED-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.

Security Objective	Type	Rationale
O.ACCOUNT-TOE: The TOE must ensure, for actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions. This will be done with moderate effectiveness, in that it is anticipated that individual accountability might not be achieved for some actions.	TOE	P.ACCOUNT T.TRACEABLE-NON-TOE T.RECORD-EVENT-NON-TOE T.AUDIT-CORRUPTED-NON-TOE
O.AUTHORIZE-Non-TOE: The IT other than the TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This is expected with a high degree of effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	Env	P.ACCESS This explicitly refers to IT other than the TOE. Hence this is environmental.
O.AUTHORIZE-TOE: The TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This will be accomplished with high effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	TOE	P.ACCESS
O.AVAILABLE-Non-TOE: The IT other than the TOE must protect itself from unsophisticated, denial-of-service attacks. This is a combination of prevention and detect and recover with a high degree of effectiveness.	Env	P.SURVIVE T.DENIAL-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.
O.AVAILABLE-TOE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection with high effectiveness.	TOE	P.SURVIVE T.DENIAL-TOE
O.BYPASS-Non-TOE: For access not controlled by the TOE, IT other than the TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because IT controls in the notional CSPP system are not expected to provide sufficient mitigation for the greater negative impact that 'malicious' implies.	Env	T.ACCESS-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.

Security Objective	Type	Rationale
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because CSPP-OS controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	TOE	T.ACCESS-TOE
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements. This will be accomplished via some technical controls, yet with a focus on non-technical controls to achieve this objective with high effectiveness.	Joint	O.COMPLY As compliance applies to the entire IT system, this requires support by the TOE, other IT, and the non-IT environment. Hence this is joint.
O.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks. The focus is on detection and response with a goal of moderate effectiveness.	Env	P.SURVIVIE T.DENIAL-SOPHISTICATED As the TOE is lower assurance IT, this objective is expected to be met primarily by the environment. Hence this is environmental.
O.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state). The goal is for moderate effectiveness.	Env	P.SURVIVE T.SYSTEM-CORRUPTED As the TOE is lower assurance IT, this objective is expected to be met primarily by the environment. Hence this is environmental.
O.DETECT-SYSTEM: The TOE, in conjunction with other IT in the system, must enable the detection of system insecurities. The goal is high effectiveness for lower grade attacks.	Joint	P.SURVIVE T.SYSTEM-CORRUPTED Being an underlying OS, the TOE is expected to help in meeting this objective. Since the TOE is lower assurance IT, significant environmental support is expected in order to accomplish this objective. Hence this is joint.
O.DETECT-TOE: The TOE must enable the detection of TOE specific insecurities. The goal is high effectiveness for lower grade attacks.	TOE	P.SURVIVE T.TOE-CORRUPTED

Security Objective	Type	Rationale
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization. This will be accomplished via a combination of technical and non-technical controls to achieve this objective with high effectiveness.	Joint	P.DUE-CARE As exercising due care applies to the entire IT system, this requires support by the TOE, other IT, and the non-IT environment. Hence this is joint.
O.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users. This will be accomplished primarily via prevention with a goal of high effectiveness. User training and awareness will provide a major part of achieving this objective.	Env	T.ENTRY-NON-TECHNICAL The nature of this threat precludes its being addressed by TOE mechanisms. Hence this is environmental.
O.ENTRY-Non-TOE: For resources not controlled by the TOE, IT other than the TOE must prevent logical entry using unsophisticated, technical methods, by persons without authority for such access. This is clearly a prevent focus and is to be achieved with a high degree of effectiveness.	Env	P.USAGE T.ENTRY-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.
O.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack. This will be accomplished by focusing on detection and response with a goal of moderate effectiveness.	Env	T.ENTRY-SOPHISTICATED As the TOE is lower assurance IT, this objective is expected to be met primarily by the environment. Hence this is environmental.
O.ENTRY-TOE: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access. This will be accomplished with high effectiveness.	TOE	P.USAGE T.ENTRY-TOE
O.INFO-FLOW: The TOE environment must ensure that any information flow control policies are enforced - (1) between system components and (2) at the system external interfaces. This will be accomplished by preventing unauthorized flows with high effectiveness.	Env	P.INFO-FLOW As near-term COTS, the TOE is not expected to provide mechanisms to help meet this objective. Hence this is environmental.
O.KNOWN-Non-TOE: The IT other than the TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This is expected with a high degree of effectiveness.	Env	P.KNOWN This explicitly refers to IT other than the TOE. Hence this is environmental.
O.KNOWN-TOE: The TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This will be accomplished with high effectiveness.	TOE	P.KNOWN

Security Objective	Type	Rationale
O.MANAGE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security. This will be accomplished with moderate effectiveness.	Joint	T.ADMIN-ERROR Being an underlying OS, the TOE is expected to help in meeting this objective. However, since this applies to the whole system, other IT is involved. Moreover, non-IT controls will likely be a major part of meeting this objective. Hence this is joint.
O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness.	Joint	P.NETWORK As this applies to the entire system, both the TOE and other IT are involved. Hence this is joint.
O.OBSERVE-Non-TOE: The IT other than the TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	Env	T.OBSERVE-NON-TOE This explicitly refers to IT other than the TOE. Hence this is environmental.
O.OBSERVE-TOE: The TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	TOE	T.OBSERVE-TOE
O.OPERATE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that the system is delivered, installed, and operated in a manner which maintains IT security. This will be accomplished with moderate effectiveness.	Joint	T.INSTALL T.OPERATE P.TRAINING Being an underlying OS, the TOE is expected to help in meeting this objective. However, since this applies to the whole system, other IT is involved. Moreover, non-IT controls will likely be a major part of meeting this objective. Hence this is joint.
O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security. This will be accomplished primarily via prevention with a goal of high effectiveness.	Env	P.PHYSICAL T.PHYSICAL Being an OS, the TOE is not expected to provide mechanisms that address this objective. Hence this is environmental.

Security Objective	Type	Rationale
O.RECOVER-SYSTEM: The system must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with some prevention and a majority of detect and respond, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	Joint	P.SURVIVE T.CRASH-SYSTEM Being an underlying OS, the TOE is expected to help in meeting this objective. However, since this applies to the whole system, other IT is involved. Moreover, non-IT controls will likely be a major part of meeting this objective. Hence this is joint.
O.RECOVER-TOE: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with a high effectiveness for specified failures and a low effectiveness for failures in general.	TOE	P.SURVIVE T.CRASH-TOE
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	TOE	P.SURVIVE T.RESOURCES Note: This objective is classed as TOE due to the fact that resource allocation mechanisms are expected to be primarily contained with in the OS.

4.0 TOE FUNCTIONAL REQUIREMENTS RATIONALE

The rationale for the set of CSPP-OS TOE functions will be based upon the following:

- Necessary – all required. Each function either (1) meets a dependency for a necessary functional or assurance requirement or (2) is required in order to meet one or more security objectives.
- Sufficient – meet objectives. The list of functions completely meets the IT security objectives and the TOE's responsibilities with respect to environmental objectives. Also, the strength of function claims are appropriate for the stated effectiveness claims.
- Correct –
  - Cover dependencies. All dependencies for each functional requirement are satisfied.
  - Operations correct. All operations on CC elements are justified and have been performed in accordance with CC guidelines and in accordance with intended CSPP purpose.
  - Deferred operations correct. All deferred operations are justified.
  - Extensions correct. All extensions to CC elements and components are justified and have been performed in accordance with CC guidelines and in accordance with intended CSPP purpose.

4.1 NECESSARY TOE FUNCTIONALITY

Table 4.1-1 provides the rationale for the necessity of each TOE functional requirement included in CSPP. Necessity is demonstrated if, for each functional requirement, there is at least one security objective that cannot be met without it. This can be achieved either by directly addressing one or more objectives or by meeting a required dependency for another functional component that directly addresses security objectives. The latter case is true for functional requirements number 3 and 37.

Function numbers missing from this table represent functions identified in [CSPP] that do not apply to this TOE.

Table 4.1-1 Necessary TOE Functionality – Mapping Function to Requirement

#	Functional Component	Name	Dependency for	Required to help address
1	FAU_GEN.1-CSPP	Audit data Generation	FAU_GEN.2 FAU_SAR.1 FAU_SEL.1-CSPP FAU_STG.1	O.ACCOUNT-TOE O.RECOVER-TOE O.RECOVER-SYSTEM O.DETECT-TOE O.DETECT O.OPERATE O.MANAGE O.DUE-CARE
2	FAU_GEN.2	User Identity Generation		O.ACCOUNT-TOE
3	FAU_SAR.1	Audit Review	FAU_SAR.2 FAU_SAR.3	
4	FAU_SAR.2	Restricted Audit Review		O.BYPASS-TOE
5	FAU_SAR.3	Selectable Audit Review		O.ACCOUNT-TOE O.RECOVER-TOE O.RECOVER-SYSTEM O.DETECT-TOE O.DETECT O.DUE-CARE O.OPERATE O.MANAGE O.COMPLY
6	FAU_SEL.1-CSPP	Selective Audit		O.DUE-CARE O.DETECT-TOE O.DETECT O.MANAGE O.OPERATE O.COMPLY

#	Functional Component	Name	Dependency for	Required to help address
7	FAU_STG.1	Protected audit trail storage	FAU_STG.3	O.DETECT-TOE O.DETECT O.DUE-CARE O.COMPLY O.ACCOUNT-TOE O.BYPASS-TOE
8	FAU_STG.3	Action in case of Possible Audit Data Loss		O.ACCOUNT-TOE O.DUE-CARE O.MANAGE
9	FDP_ACC.1	Subset Access Control	FDP_ACF.1-CSPP FDP_ETC.1-CSPP FDP_ITC.1 FDP_ITT.1 FDP_UCT.1 FDP_UIT.1 FMT_MSA.1	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-TOE O.RESOURCES
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	FDP_ACC.1	O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE O.COMPLY O.AVAILABLE-TOE O.RESOURCES
12	FDP_ETC.1-CSPP	Export of user data without security attributes		O.BYPASS-TOE O.DUE-CARE O.ENTRY-TOE O.AVAILABLE-TOE
15	FDP_ITC.1	Import of user data without security attributes		O.NETWORK
17	FDP_RIP.1	Subset Residual Information protection		O.BYPASS-TOE O.DUE-CARE
19	FDP_UCT.1	Basic data exchange confidentiality		O.NETWORK
20	FDP_UIT.1	Data exchange integrity		O.NETWORK
21	FIA_AFL.1	Authentication Failure Handling		O.DETECT-TOE O.DETECT O.ENTRY-TOE O.BYPASS-TOE O.DUE-CARE O.COMPLY
22	FIA_ATD.1	User Attribute Definition	FIA_USB.1	O.AUTHORIZE-TOE

#	Functional Component	Name	Dependency for	Required to help address
23	FIA_SOS.1	Verification of Secrets		O.BYPASS-TOE O.DUE-CARE O.COMPLY
25	FIA_UAU.1	Timing of authentication	FIA_AFL.1 FIA_UAU.7 FTA_SSL.1 FTA_SSL.2	O.KNOWN-TOE
26	FIA_UAU.5	Multiple authentication mechanisms		O.NETWORK
27	FIA_UAU.6	Re-authenticating		O.BYPASS-TOE
28	FIA_UAU.7	Protected authentication feedback		O.BYPASS-TOE
29	FIA_UID.1	Timing of identification	FAU_GEN.2 FIA_UAU.1 FMT_SMR.1 FTA_MCS.1-CSPP	O.KNOWN-TOE
30	FIA_USB.1	User-Subject Binding		O.ACCESS-TOE O.ACCESS-MALICIOUS O.DUE-CARE O.BYPASS-TOE
31	FMT_MOF.1	Management of security functions behavior		O.MANAGE O.DUE-CARE
32	FMT_MSA.1	Management of security attributes	FMT_MSA.3	O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE
33	FMT_MSA.3	Static attribute initialization	FDP_ACF.1-CSPP FDP_IFF.1 FDP_IFF.8 FDP_ITC.1	O.MANAGE O.DUE-CARE O.AUTHORIZE-TOE
34	FMT_MTD.1	Management of TSF data	FAU_SEL.1-CSPP	O.MANAGE O.DUE-CARE
35	FMT_SAE.1	Time-Limited Authorization		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.AUTHORIZE-TOE O.MANAGE O.DUE-CARE

#	Functional Component	Name	Dependency for	Required to help address
36	FMT_SMR.1	Security roles	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_MTD.1 FMT_SAE.1	O.MANAGE O.DUE-CARE
37	FPT_AMT.1	Abstract Machine Testing	FPT.TST.1	
38	FPT_FLS.1	Failure with preservation of secure state		O.RECOVER-TOE O.RECOVER-SYSTEM
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission		O.NETWORK
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification		O.NETWORK
42	FPT_RCV.2	Automated Recovery		O.RECOVER-TOE O.RECOVER-SYSTEM
43	FPT_RPL.1-CSPP	Replay detection		O.NETWORK
44	FPT_RVM.1	Non-Bypassability of the TSP		O.BYPASS-TOE
45	FPT_SEP.1	TSF Domain Separation		O.BYPASS-TOE O.DUE-CARE
46	FPT_TDC.1	Inter-TSF basic TSF data consistency		O.NETWORK
48	FPT_TST.1	TSF Testing	FPT_RCV.1	O.DETECT-TOE O.DETECT O.DUE-CARE
49	FRU_RSA.1	Maximum quotas		O.RESOURCES
50	FTA_LSA.1	Limitation on scope of selectable attributes		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE O.DUE-CARE
52	FTA_SSL.1	TSF-initiated session locking		O.BYPASS-TOE O.DUE-CARE
53	FTA_SSL.2	User-initiated locking		O.OPERATE O.BYPASS-TOE O.DUE-CARE
54	FTA_SSL.3	TSF-initiated termination		O.BYPASS-TOE O.DUE-CARE

#	Functional Component	Name	Dependency for	Required to help address
55	FTA_TAB.1-CSPP	Default TOE access banners		O.ENTRY-TOE O.ACCOUNT-TOE O.DUE-CARE O.COMPLY
56	FTA_TAH.1	TOE access history		O.OBSERVE-TOE O.ENTRY-TOE O.BYPASS-TOE O.DUE-CARE O.COMPLY
57	FTA_TSE.1	TOE session establishment		O.ACCESS-TOE O.ACCESS-MALICIOUS O.ENTRY-TOE
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	FDP_UCT.1 FDP_UIT.1	O.NETWORK
59	FTP_TRP.1-CSPP	Trusted path	FDP_UCT.1 FDP_UIT.1	O.NETWORK
60	Non-CC FPT_SYN-CSPP.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	FPT_GEN.1 FMT_SAE.1	O.NETWORK

4.2 SUFFICIENT TOE FUNCTIONALITY

4.2.1 Coverage of Security Objectives

Table 4.2-1 indicates completeness of the functional set with respect to covering each TOE security objective. As the assurance level for this PP (EAL2) is low, the rigor required to justify coverage is also low and is provided in the form of a list of functions for each objective.

Table 4.2-2 maps Joint security objectives to TOE security functions, identifying the TOE portion of meeting that objective.

Table 4.2-1 Complete Functionality - Map TOE Security Objective to TOE Functionality

Security Objective	TOE Functionality
O.ACCESS-TOE: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized. This will be accomplished with high effectiveness.	9 FDP_ACC.1 10 FDP_ACF.1-CSPP 30 FIA_USB.1 35 FMT_SAE.1 50 FTA_LSA.1 51 FTA_MCS.1-CSPP 57 FTA_TSE.1
O.ACCOUNT-TOE: The TOE must ensure, for actions under its control or knowledge, that all TOE users can subsequently be held accountable for their security relevant actions. This will be done with moderate effectiveness, in that it is anticipated that individual accountability might not be achieved for some actions.	1 FAU_GEN.1-CSPP 2 FAU_GEN.2 5 FAU_SAR.3 7 FAU_STG.1 8 FAU_STG.3 55 FTA_TAB.1-CSPP
O.AUTHORIZE-TOE: The TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements under its control, supporting the organization's security policy for access control. This will be accomplished with high effectiveness. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	22 FIA_ATD.1 32 FMT_MSA.1 33 FMT_MSA.3 35 FMT_SAE.1
O.AVAILABLE-TOE: The TOE must protect itself from unsophisticated, denial-of-service attacks. This will include a combination of protection and detection with high effectiveness.	9 FDP_ACC.1 10 FDP_ACF.1-CSPP 12 FDP_ETC.1-CSPP

Security Objective	TOE Functionality
O.BYPASS-TOE: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement. This will be accomplished with high effectiveness. NOTE: This objective is limited to 'non-malicious' because CSPP-OS controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	4 FAU_SAR.2 7 FAU_STG.1 12 FDP_ETC.1-CSPP 17 FDP_RIP.1 21 FIA_AFL.1 23 FIA_SOS.1 27 FIA_UAU.6 28 FIA_UAU.7 30 FIA_USB.1 44 FPT_RVM.1 45 FPT_SEP.1 52 FTA_SSL.1 53 FTA_SSL.2 54 FTA_SSL.3 56 FTA_TAH.1
O.DETECT-TOE: The TOE must enable the detection of TOE specific insecurities. The goal is high effectiveness for lower grade attacks.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 6 FAU_SEL.1-CSPP 7 FAU_STG.1 21 FIA_AFL.1 48 FPT_TST.1
O.ENTRY-TOE: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access. This will be accomplished with high effectiveness.	9 FDP_ACC.1 10 FDP_ACF.1-CSPP 12 FDP_ETC.1-CSPP 21 FIA_AFL.1 35 FMT_SAE.1 50 FTA_LSA.1 51 FTA_MCS.1-CSPP 55 FTA_TAB.1-CSPP 56 FTA_TAH.1 57 FTA_TSE.1
O.KNOWN-TOE: The TOE must ensure that, for all actions under its control and except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access. This will be accomplished with high effectiveness.	25 FIA_UAU.1 29 FIA_UID.1
O.OBSERVE-TOE: The TOE must ensure that its security status is not misrepresented to the administrator or user. This is a combination of prevent and detect and, considering the potentially large number of possible failure modes, is to be achieved with a moderate, verses high, degree of effectiveness.	56 FTA_TAH.1

Security Objective	TOE Functionality
O.RECOVER-TOE: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with a high effectiveness for specified failures and a low effectiveness for failures in general.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 38 FPT_FLS.1 42 FPT_RCV.2
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion. This will be accomplished via protection with high effectiveness.	9 FDP_ACC.1 10 FDP_ACF.1-CSPP 49 FRU_RSA.1

Table 4.2-2 Complete Functionality - Map Joint Security Objective to TOE Functionality

Security Objective	TOE Functionality
O.ACCESS-MALICIOUS: The TOE controls will help in achieving this objective, but will not be sufficient. Additional, environmental controls are required to sufficiently mitigate the threat of malicious actions by authenticated users. This will be accomplished by focusing on deterrence, detection, and response with a goal of moderate effectiveness.	9 FDP_ACC.1 10 FDP_ACF.1-CSPP 30 FIA_USB.1 35 FMT_SAE.1 50 FTA_LSA.1 51 FTA_MCS.1-CSPP 57 FTA_TSE.1
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements. This will be accomplished via some technical controls, yet with a focus on non-technical controls to achieve this objective with high effectiveness.	5 FAU_SAR.3 6 FAU_SEL.1-CSPP 7 FAU_STG.1 9 FDP_ACC.1 10 FDP_ACF.1-CSPP 21 FIA_AFL.1 23 FIA_SOS.1 55 FTA_TAB.1-CSPP 56 FTA_TAH.1
O.DETECT-SYSTEM: The TOE, in conjunction with other IT in the system, must enable the detection of system insecurities. The goal is high effectiveness for lower grade attacks.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 6 FAU_SEL.1-CSPP 7 FAU_STG.1 21 FDP_AFL.1 48 FPT_TST.1

Security Objective	TOE Functionality
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization. This will be accomplished via a combination of technical and non-technical controls to achieve this objective with high effectiveness.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 6 FAU_SEL.1-CSPP 7 FAU_STG.1 8 FAU_STG.3 9 FDP_ACC.1 10 FDP_ACF.1-CSPP 12 FDP_ETC.1-CSPP 17 FDP_RIP.1 21 FIA_AFL.1 23 FIA_SOS.1 30 FIA_USB.1 31 FMT_MOF.1 32 FMT_MSA.1 33 FMT_MSA.3 34 FMT_MTD.1 35 FMT_SAE.1 36 FMT_SMR.1 45 FPT_SEP.1 48 FPT_TST.1 50 FTA_LSA.1 51 FTA_MCS.1-CSPP 52 FTA_SSL.1 53 FTA_SSL.2 54 FTA_SSL.3 55 FTA_TAB.1-CSPP 56 FTA_TAH.1

Security Objective	TOE Functionality
O.MANAGE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security. This will be accomplished with moderate effectiveness.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 6 FAU_SEL.1-CSPP 8 FAU_STG.3 31 FMT_MOF.1 32 FMT_MSA.1 33 FMT_MSA.3 34 FMT_MTD.1 35 FMT_SAE.1 36 FMT_SMR.1
O.NETWORK: The system must be able to meet its security objectives in a distributed environment. This will be accomplished with high effectiveness.	15 FDP_ITC.1 19 FDP_UCT.1 20 FDP_UIT.1 26 FIA_UAU.5 39 FPT_ITC.1-CSPP 40 FPT_ITI.1-CSPP 43 FPT_RPL.1-CSPP 46 FPT_TDC.1 58 FTP_ITC.1-CSPP 59 FTP_TRP.1-CSPP 60 FPT_SYN-CSPP.1
O.OPERATE: Those responsible for the system (in conjunction with mechanisms provided by the TOE) must ensure that the system is delivered, installed, and operated in a manner which maintains IT security. This will be accomplished with moderate effectiveness.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 6 FAU_SEL.1-CSPP 53 FTA_SSL.2
O.RECOVER-SYSTEM: The system must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity. This will be accomplished with some prevention and a majority of detect and respond, with high effectiveness for specified failures. For general failure, this will be accomplished with low effectiveness.	1 FAU_GEN.1-CSPP 5 FAU_SAR.3 38 FPT_FLS.1 42 FPT_RCV.2

4.2.2 Strength of Function (SOF)

4.2.2.1 Minimum SOF Claim

The basic design goal for CSPP was to produce a requirement set that is suitable for near-term implementation with commercial off the shelf products. The selection of ***basic*** as the minimum level is clearly a direct result of this goal.

4.2.2.2 Specific SOF Claims

The specific SOF claims are all within the category of currently, and widely available. All represent at least a ***basic*** level of strength.

Note that, while not probabilistic, SOF metrics have been given for FAU_STG.1, FDP_RIP.1, FMT_MTD.1, and FPT_SEP.1. This extension of the CC with respect to SOF, is being used as a convenient means of capturing all “strength” elements in a common location of the PP.

4.3 CORRECT TOE FUNCTIONALITY

4.3.1 Dependencies for TOE functionality

Table 4.3.1-1 shows correctness of the TOE functional set with respect to meeting all dependencies. (Missing function numbers represent functions called out in [CSPP] that do not apply to this TOE.)

Table 4.3.1-1 Correct TOE Functionality – Dependency Mapping

#	CSPP Functional Component	Name	Dependency	CSPP-OS TOE Function #
1	FAU_GEN.1-CSPP	Audit data Generation	FPT_SYN-CSPP.1	60
2	FAU_GEN.2	User Identity Generation	FAU_GEN.1-CSPP FIA_UID.1	1 29
3	FAU_SAR.1	Audit Review	FAU_GEN.1-CSPP	1
4	FAU_SAR.2	Restricted Audit Review	FAU_SAR.1	3
5	FAU_SAR.3	Selectable Audit Review	FAU_SAR.1	3
6	FAU_SEL.1-CSPP	Selective Audit	FAU_GEN.1-CSPP FMT_MTD.1	1 34
7	FAU_STG.1	Protected audit trail storage	FAU_GEN.1-CSPP	1
8	FAU_STG.3	Action in case of Possible Audit Data Loss	FAU_STG.1	7
9	FDP_ACC.1	Subset Access Control	FDP_ACF.1-CSPP	10
10	FDP_ACF.1-CSPP	Security Attribute Based Access Control	FDP_ACC.1 FMT_MSA.3	9 33
12	FDP_ETC.1-CSPP	Export of user data without security attributes	FDP_ACC.1 FDP_IFC.1	9 14
15	FDP_ITC.1	Import of user data without security attributes	FDP_ACC.1 FDP_IFC.1 FMT_MSA.3	9 14 33
17	FDP_RIP.1	Subset Residual Information protection	none	—
19	FDP_UCT.1	Basic data exchange confidentiality	FTP_ITC.1-CSPP FTP_TRP.1-CSPP FDP_ACC.1 FDP_IFC.1	58 59 9 13

#	CSPP Functional Component	Name	Dependency	CSPP-OS TOE Function #
20	FDP_UIT.1	Data exchange integrity	FTP_ITC.1-CSPP FTP_TRP.1-CSPP FDP_ACC.1 FDP_IFC.1	58 59 9 13
21	FIA_AFL.1	Authentication Failure Handling	FIA_UAU.1	25
22	FIA_ATD.1	User Attribute Definition	none	—
23	FIA_SOS.1	Verification of Secrets	none	—
25	FIA_UAU.1	Timing of authentication	FIA_UID.1	29
26	FIA_UAU.5	Multiple authentication mechanisms	none	—
27	FIA_UAU.6	Re-authenticating	none	—
28	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	25
29	FIA_UID.1	Timing of identification	none	—
30	FIA_USB.1	User-Subject Binding	FIA_ATD.1	23
31	FMT_MOF.1	Management of security functions behavior	FMT_SMR.1	36
32	FMT_MSA.1	Management of security attributes	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1	9 13 36
33	FMT_MSA.3	Static attribute initialization	FMT_MSA.1 FMT_SMR.1	32 36
34	FMT_MTD.1	Management of TSF data	FMT_SMR.1	36
35	FMT_SAE.1	Time-Limited Authorization	FMT_SMR.1 FMT_CSPP.1	36 60
36	FMT_SMR.1	Security roles	FIA_UID.1	29
37	FPT_AMT.1	Abstract Machine Testing	none	—
38	FPT_FLS.1	Failure with preservation of secure state	ADV_SPM.1	PP Sec 6.0
39	FPT_ITC.1-CSPP	Inter-TSF Confidentiality During Transmission	none	—
40	FPT_ITI.1-CSPP	Inter-TSF detection of modification	none	—
42	FPT_RCV.2	Automated Recovery	ADV_SPM.1 AGD_ADM.1 FPT_TST.1	PP Sec 6.0 PP Sec 6.0 48
43	FPT_RPL.1-CSPP	Replay detection	none	—
44	FPT_RVM.1	Non-Bypassability of the TSP	none	—
45	FPT_SEP.1	TSF Domain Separation	none	—
46	FPT_TDC.1	Inter-TSF basic TSF data consistency	none	—

#	CSPP Functional Component	Name	Dependency	CSPP-OS TOE Function #
48	FPT_TST.1	TSF Testing	FPT_AMT.1	37
49	FRU_RSA.1	Maximum quotas	none	—
50	FTA_LSA.1	Limitation on scope of selectable attributes	none	—
51	FTA_MCS.1-CSPP	Basic limitation on multiple concurrent session	FIA_UID.1	29
52	FTA_SSL.1	TSF-initiated session locking	FIA_UAU.1	25
53	FTA_SSL.2	User-initiated locking	FIA_UAU.1	25
54	FTA_SSL.3	TSF-initiated termination	none	—
55	FTA_TAB.1-CSPP	Default TOE access banners	none	—
56	FTA_TAH.1	TOE access history	none	—
57	FTA_TSE.1	TOE session establishment	none	—
58	FTP_ITC.1-CSPP	Inter-TSF trusted channel	none	—
59	FTP_TRP.1-CSPP	Trusted path	none	—
60	FPT_SYN-CSPP.1	TSF synchronization	none	—

4.3.2 Functional Operations

Table 4.3.2-1 provides a rationale for most completed selections, refinements, and assignments.

Table 4.3.2-2 provides the rationale for most deferred operations and related, completed operations.

Table 4.3.2-3 provides the rationale for functional extensions, and related deferred operations.

Table 4.3.2-1 Correct Functionality – Rationale for assignment, Selection, and Refinement

Assignment, Selection, and Refinement Performed	Rationale
FAU_GEN.1.1 b) All auditable events relevant for the [**selection:** basic] level of audit; and	• Basic is an appropriate level for a COTS baseline requirement set
c) [**assignment:** (1) for FPT_ITI.1 and FPT_RPL.1, the ability to provide statistical data representing the frequency of occurrence …	• In order to see patterns of network activity, it is necessary to be able to represent the statistical nature of integrity and replays - as these may be due to network performance issues and not due to attacks.
FAU_GEN.1.2 a) Date and time of the event, type of event, subject identity (human user/software process), and the outcome (success or failure) of the event; and	• Clarify that process as well as human user is to be identified.
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**assignment:** "none"].	• No further assignment is necessary.
FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the individual identity of the user or system process that caused the event.	• Clarify that process as well as human user is to be identified.
FAU_SAR.1.1 The TSF shall provide [**assignment:** explicitly authorized user roles, user groups, or individually identified users] with the capability to read [**assignment:** all information in the audit records] from the audit records.	• It is within the scope of COTS to provide the granularity of authorization in this assignment. • As a baseline, it is considered reasonable to allow reading of audit information.
FAU_SAR.3.1 The TSF shall provide the ability to perform [**selection:** searches, sorting, and ordering] of audit data based upon [**assignment:** at a minimum, date and time of the event, subject (user or process), type of event, and success or failure].	• All three CC options for the selection are appropriate. • A minimal set of rules is provided, which is considered within scope for COTS.
FAU_SEL.1.1 a) [**selection:** Object identity, user identity, subject identity, host identity, and/or event type]; b) [**assignment:** success or failure.]	• All CC options are appropriate for this selection. • These are the essential other elements to be recorded.
FAU_STG.1.2 The TSF shall be able to [**selection:** prevent and detect] modifications to the audit records.	• Want, in the baseline requirement, mechanisms to both prevent and detect.
FAU_STG.3.1 The TSF shall take [**assignment:** the action to notify an identified user or console of the possible audit data loss] if the audit trail exceeds [**assignment:** an authorized user selectable, pre-defined limit].	• This is considers a reasonable, baseline requirement. • It is considered more reasonable to make this a parameter than a fixed value.
FDP_ACC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] on [**assignment:** all subjects, all operating system controlled files (to include all communications mechanisms – for internal or external communications – that are implemented as objects controlled by the file system), and all access requests to these files].	• This is the SFP to be enforced. • The COTS OS will likely be able to accomplish this scope of access control.

Assignment, Selection, and Refinement Performed	Rationale
FDP_ACF.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to objects based on [**assignment:** user/process identity, group membership, subject privileges, and, if included in the object authorization information, access restrictions such as the time-of-day and port-of-entry].	• This the SFP to be enforced. • This assignment is considered within scope for near-term COTS products.
FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [**assignment:** by checking the authorizations associated with the object for the entries of that subject].	• Further information does not seem needed, in light of that provided with the SFP description.
FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**assignment:** none].	• None appear to be needed.
FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules:[**assignment:** none].	• Refinement is strictly editorial. • None appear to be needed.
FDP_ETC.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] when exporting user data, controlled under the SFP(s), outside of the TSC.	• This is the SFP to be enforced.
FDP_ITC.1.1 The TSF shall enforce the [**assignment:** CSPP access control] when importing user data, controlled under the SFP, from outside the TSC.	• This is the SFP to be enforced.
FDP_ITC.1.3 The TSF shall enforce the following the following rules when importing user data controlled under the SFP from outside the TSC: [**assignment:** the TOE shall provide for incoming information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access].	• This is a reasonable expectation for COTS.
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a … [**assignment:** shared memory and file storage space].	• These are the shared resources in a typical OS.
FDP_UCT.1.1 The TSF shall support the enforcement of the [**assignment:** CSPP access control SFP] to be able to [**selection:** transmit and receive] objects in a manner protected from unauthorized disclosure.	• The OS can support but not fully enforce. • This is the SFP to be enforced. • Both CC choices are appropriate here.
FDP_UIT.1.1 The TSF shall support the enforcement of the [**assignment:** CSPP access control SFP] to be able to [**selection:** transmit and receive] user data in a manner protected from [**selection:** modification, deletion, insertion, and replay] errors.	• The OS can support but not fully enforce. • This is the SFP to be enforced. • Both CC choices are appropriate here. • All CC choices are appropriate here.

Assignment, Selection, and Refinement Performed	**Rationale**
FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [**selection:** modification, deletion, insertion, or replay] has occurred.	• All four CC choices are considered appropriate.
FIA_AFL.1.1 The TSF shall detect when [**assignment:** an authorized user configurable number of] unsuccessful authentication attempts over an authorized user configurable length of time occur related to [**assignment:** initial account login, re-authentication after initial login, and *…]*].	• It is desired that this be configurable, rather than a number set in the PP. • Some time period seems to be appropriate. • These are the typical events that need to be covered. The remainder of the assignment is covered under 'deferred operations'.
FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment**: for passwords, the application note below and the requirements of FIPS PUB 112; for other …	• This is considered reasonable for passwords. The remainder of the assignment is covered under 'deferred operations'.
FIA_UAU.1.1 The TSF shall allow [**assignment:** no actions other than anonymous access to resources explicitly authorized for the type of anonymous access requested and …	• This is the basic statement of need.
FIA_UAU.5.1 The TSF shall provide support for [**assignment:** the required use of authentication mechanisms other than only passwords, based upon access parameters such as time of day, port of entry, and user privilege] to support user authentication.	• OS must support, not necessary fully provide. • This is a general statement of the desired need.
FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**assignment:** parameters for selecting authenticators required, these parameters are to be specifiable by an explicitly specified set of users, enforcing least privilege on the basis of …	• This is a general statement of the desired need. The remainder of the assignment is covered under 'deferred operations'.
FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**assignment:** re-establishing a session following session locking, request to change authentication secrets, and …	• These are the basic needs for re-authentication. Other needs are addressed in the deferred operation.
FIA_UAU.7.1 The TSF shall not provide [**assignment:** any indication of success or failure nor clear-text display of any secret authenticator] to the user while the authentication is in progress.	• Refinement recasts requirement in the negative as that is the primary need here. • This is a reasonable, common requirement.
FIA_UID.1.1 The TSF shall allow [**assignment:** no actions other than anonymous access to resources explicitly authorized for the type of anonymous access requested and …	• This is the basic statement of need.
FMT_MOF.1.1 The TSF shall restrict the ability to [**selection:** determine the behaviour of, disable, enable, modify the behavior of] the functions [**assignment:** included as requirements for CSPP-OS and for which the common criteria indicates security management suggestions, and …	• All four CC choices are appropriate. • The CC suggestions will be followed. Other needs are addressed in the deferred operation.
FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to restrict the ability to [**selection:** change_default, modify, delete] and [**assignment:** "null"] the security attributes [**assignment:** all attributes used to define the	• This is the SFP to be enforced. • All CC choices, except query are appropriate, with no additional options per the assignment.

Assignment, Selection, and Refinement Performed	Rationale
security state of the system, to control the security functionality, to make access control decisions, and … to [**assignment:** for discretionary attributes, the owner of the attribute; for both discretionary and non-discretionary attributes, an explicitly specified set of users, …]. … See iteration for restriction on read access to authenticator values.	Query is handled by iteration, see below. • The refinement "and" is editorial. • This provides the description of the need. Additional details are covered in the deferred operation. • This is considered an appropriate statement of the need.
Iteration: FMT_MSA.1.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to restrict the ability to [**selection:** query] [**assignment:** "null"] the security attributes [**assignment:** current and past values of authenticators,] to [**assignment:** no users and only to software processes requiring this knowledge].	• The refinement clarifies the use of iteration. • This is the SFP to be enforced. • The issue here is reading. • The values of concern are authenticators. • This information is not provided to the human interface and is limited to explicitly authorized processes.
FMT_MSA.3.1 The TSF shall enforce the [**assignment:** CSPP access control SFP] to provide [**assignment:** restrictive] default values for object security attributes that are used to enforce the SFP.	• This is the SFP to be enforced. • A restrictive default is desired.
FMT_MSA.3.2 The TSF shall allow the [**assignment:** data object owner and other authorized users] to specify alternate initial values to override the default values when an object or information is created.	• The owner and privileged users should be able to assign these values.
FMT_MTD.1.1 The TSF shall restrict the ability to [**selection:** change_default, read, modify, delete, or clear] the [**assignment:** all internal TSF data structures that are security critical] to [**assignment:** software processes explicitly authorized to access this data].	• All CC selections are appropriate. • This is a general description of the scope. • Explicit authorization is required.
FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [**assignment:** user account and authenticators and …	• This is a basic set of actions to be covered. Additional actions are covered by the deferred operation.
FMT_SAE.1.2 For each of these security attributes, TSF shall be able to [**assignment:** for user account - disable account and require administrator action to re-enable, for authenticators - require owner of authenticator to establish a new value before proceeding with authenticated action] and …	• This requires explicit specification which is accomplished in conjunction with the deferred operation. • This is considered a reasonable baseline requirement. Additional details are covered by the deferred operation.
FMT_SMR.1.1 The TSF shall maintain the roles [**assignment:** privileged user (for example the equivalent of the Unix root) and/or …	• This is a reasonable baseline requirement with additional possibilities through the deferred operation.
FPT_AMT.1.1 The TSF shall run a suite of tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)] to demonstrate the correct operation of the security assumptions provided by the abstract machine which underlies the TSF.	• These two CC selections are considered minimal. • Providing clarification for "authorized user".
FPT_ITC.1.1-CSPP The TSF shall support the protection of …	

Assignment, Selection, and Refinement Performed	Rationale
transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.	• The OS can support, but may not be able to fully implement this function.
FPT_ITI.1.1-CSPP The TSF shall support the capability to detect modification of …	• The OS can support, but may not be able to fully implement this function.
FPT_ITI.1.2-CSPP The TSF shall support the capability to verify the integrity of … transmitted between the TSF and a remote trusted IT product and perform [**assignment:** automatic retransmission of data lacking integrity, with the capability to audit this action in a statistical manner] if modifications are detected. ...	• The OS can support, but may not be able to fully implement this function. • This is the most practical response.
FPT_RPL.1.2 The TSF shall perform [**assignment:** the action of discarding duplicates and providing the capability to audit this action in a statistical manner] when replay is detected.	• This is the most practical response.
FPT_RVM.1.1 The TSF shall ensure, to at least a level of confidence appropriate for a lower-level of assurance (i.e., EAL-CSPP), that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.	• This refinement clarifies the degree of confidence expected in this open-ended requirement.
FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects, at least to the extent such protection can be reasonably expected from a lower-level of assurance (i.e., EAL-CSPP), it from interference and tampering by untrusted subjects.	• This refinement clarifies the degree of confidence expected in this open-ended requirement.
Refinement: FPT_TDC.1.3-CSPP The TSF shall support maintaining consistent data between this TSF and another trusted IT product for the data items specified in FPT_TDC.1.1 in accordance with the rules specified in FPT_TDC.1.2.	• This is a refinement, as the new element only clarifies the intent of the component. The CC component imposes requirements related to consistent syntax and interpretation, but does not, as this new element adds, require mechanisms to ensure that information is kept current and consistent between trusted products.
FPT_TST.1.1 The TSF shall run a suite of self tests [**selection:** during initial start-up and at the request of explicitly authorized security administrator(s) or security administrator role(s)] [**assignment:** "null"] to demonstrate the correct operation of the TSF.	• These two CC selections are considered minimal. • Providing clarification for "authorized user". • No other conditions are required in the baseline specification.
FRU_RSA.1.1-CSPP The TSF shall enforce maximum quotas of the following resources: [**assignment:** all OS-controlled, multi-user or multi-process resources such as memory, disk space, and inter-processor communications paths] that …	• These are the basic shared resources.
FTA_MCS.1.2 If the TOE is to restrict the maximum number of concurrent sessions, the TSF shall enforce [**assignment:** an authorized user selected maximum number of] sessions per user.	• Refinement clarifies intent with extended element.
FTA_SSL.1.1 The TSF shall lock an interactive session after	• Consider it better to make this a parameter

Assignment, Selection, and Refinement Performed	Rationale
[**assignment:** an authorized user specified time interval of user inactivity] …	rather than a specified number.
FTA_SSL1.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].	• Consider it better to make this a parameter rather than a specified number.
FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [**assignment:** user authentication].	• This is the baseline need.
FTA_SSL.3.1 The TSF shall terminate an interactive session after [**assignment:** an authorized user specified time interval of user inactivity].	• This is the baseline need.
FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [**selection:** date, time, method, <u>and</u> location] of the last successful session establishment to the user.	• Consider it better to make this a parameter rather than a specified number.
FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [**selection:** date, time, method, <u>and</u> location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.	• All four CC choices are appropriate. • All four CC choices are appropriate.
FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment:** attributes that can be set by explicitly authorized security administrator(s) or security administrator role(s), including user identity, port of entry, time of day, day of the week, and …	• These are the basic elements upon which session denial might be based.
FTP_TRP.1.1-CSPP The TSF shall provide a communication path between itself and [**selection:** local] users …	
FTP_TRP.1.2 The TSF shall permit [**selection:** local users] to initiate communication via the trusted path. <u>(Note that this requirement does not prevent the TSF from initiating communications, only that the TOE must allow local users to do so.)</u>	• 'Local' is the reasonable expectation for near-term COTS. • These choices are the reasonable ones for near-term COTS.
FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**selection:** initial user authentication,] [**assignment:** user re-authentication, and …	• The refinement clarifies the intent of this requirement in CSPP-OS. • These two choices are the ones mostly likely to be applicable. (The deferred assignment provides for the possibility of more.)

Table 4.3.2-2 Correct Functionality – Rationale for Deferring Operations to ST

Functional Operations Deferred to ST	Rationale for Deferring to ST
FAU_GEN.1.1 c) [**assignment:** (2) other auditable events specific to the ST design as listed in the following ST assignment: *[**ST assignment:** any other audit events required by specifics of the ST design in order to meet PP requirements*.] The ST rationale shall provide a basic justification, showing that the ST assignment, to include a "null" assignment, is complete.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • By requiring justification from the ST author, the validity of the completion can be determined.
FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [**assignment:** following: *[**ST selection:** allocation of the resource to, deallocation of the resource from, both]*] the following objects …. The ST rationale shall provide a basic justification, showing that the ST selection is consistent with other aspects of the ST design, resulting in a secure solution.	• It does not matter at the PP level of abstraction which is selected, as long as the selection is not contrary to specifics of the ST design. • The ST author is required to justify the selection made.
FIA_AFL.1.1 The TSF shall detect when … occur related to [**assignment:** …, and list of other events given in the following ST assignment: *[**ST assignment:** as required by PP, list of ST specific authentication events]*]. The ST rationale shall provide a basic justification that the ST assignment, including a "null" assignment, includes all events specific to the ST design that require authentication failure handling.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • By requiring justification from the ST author, the validity of the completion can be determined.
FIA_AFL.1.2 After the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [**assignment:** perform the following ST selected actions: *[**ST selection:** disable the account (requiring it to be re-enabled by an authorized user), cause each subsequent logon attempt to be delayed for increasing periods of time up to a maximum number of additional attempts at which time the account is disabled pending authorized user action to re-enable, allow either option based upon a configuration choice by an authorized user]*]. As any selection, other than "null", is acceptable and the purpose here is to ensure that an explicit choice is both made and announced, the ST rationale need not justify the choice made.	• It is considered necessary to know the capabilities of the TOE, but not to specify which action(s) are provided, as long as at least one is present. (The set of choices provided represents commonly available choices.) • The refinement defines what is expected with respect to ST justification.
FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**assignment:** user name, authenticator and the following ST specific attributes required by the design of the ST: *[**ST assignment:** as required by PP, list of any ST specific security attributes]*]. The ST rationale shall provide a basic justification for the assignment made, including "null", showing that it is the complete list required to maintain secure operation.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • By requiring justification from the ST author, the validity of the completion can be determined.
FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**assignment**: …; for other secrets specific to the ST design, the metrics called out in the following ST assignment: *[**ST assignment:** as required by PP, any ST*	• The ST will provide information about the security functions and mechanisms not available to the PP author.

Functional Operations Deferred to ST	Rationale for Deferring to ST
specific, defined quality metrics]]. The ST rationale shall provide a basic justification that the ST assignment covers all ST specific secrets essential for secure operation and that the metric(s) given are appropriate for meeting the PP design goals.	• By requiring justification from the ST author, the validity of the completion can be determined.
FIA_UAU.1.1 The TSF shall allow [**assignment:** … and the following ST selection *[**ST selection:** as permitted by PP, local shut down of the operating system]*] on behalf of the user to be performed before the user is authenticated. As the inclusion of this action is permitted, but not required, and the purpose here is only to ensure that the ST choice is explicit, the ST rationale does not need to include a justification for the choice made.	• It is considered sufficient to know whether the action listed is present in the TOE. • This defines what justification is to be provided by the ST author.
FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**assignment:** …, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** explicitly authorized security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic justification for the selection made, indicating how it supports enforcement of least privilege.	• Specifics of the TOE design may result in a preferred choice for the selection. • At the level of abstraction of the PP any selection is acceptable provided it is justified in the ST.
FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**assignment:** …, and the following ST supplied conditions specific to the ST design: *[**ST assignment:** as required by PP, list of other, ST specific conditions under which re-authentication is required]*]. The ST rationale shall provide a basic justification for the assignment made, including a "null" list, showing why it is complete.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • By requiring justification from the ST author, the validity of the completion can be determined.
FIA_UID.1.1 The TSF shall allow [**assignment:** … and the following ST selection *[**ST selection:** as allowed by PP, local shut down of the operating system]*] on behalf of the user to be performed before the user is identified. As the operation is permitted rather than required, and the purpose here is to ensure that the choice is explicit, the ST rationale does not need to include a justification for the choice made.	• It is considered sufficient to know whether the action listed is present in the TOE. • This defines what justification is to be provided by the ST author.
FMT_MOF.1.1 The TSF shall restrict the ability to … the functions [**assignment:** …, and also all items listed in the following ST assignment: *[**ST assignment:** as required by PP, list of ST functions and mechanisms resulting from specifics of the ST design]*] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale must provide a basic justification for the assignment made, to include "null". The ST rationale must also provide a basic justification for the selection made, indicating how it supports enforcement of least privilege.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • Specifics of the TOE design may result in a preferred choice for the selection. • This defines what justification is to be provided by the ST author.
FMT_MSA.1.1 The TSF shall enforce the … the security attributes [**assignment:** …, and those listed in the following ST assignment: *[**ST assignment:** as required by PP, list of security attributes requiring management and arising from the specifics*	• The ST will provide information about the security functions and mechanisms not available

Functional Operations Deferred to ST	**Rationale for Deferring to ST**
of the ST design]] to [**assignment:** for discretionary attributes, the owner of the attribute; for both discretionary and non-discretionary attributes, an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: and *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic rationale for the assignment made, showing it to be complete. Also, the ST rationale shall provide a basic justification for the selection made, indicating how it enforces least privilege. …	to the PP author. • Specifics of the TOE design may result in a preferred choice for the selection. • This defines what justification is to be provided by the ST author
FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [**assignment:** … and *[**ST assignment:** as required by PP, list of ST specific security attributes for which expiration is to be supported]*] to [**assignment:** an explicitly specified set of users, enforcing least privilege on the basis of the following ST selection: *[**ST selection:** security administrators, security administrator roles, both]*]. The ST rationale shall provide a basic justification for the assignment made, to include a “null” assignment, showing that it is a complete list with respect to the attributes which must be restricted to enforce secure operation. The ST rationale shall also provide a basic justification for the selection made, indicating how it enforces least privilege.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • Specifics of the TOE design may result in a preferred choice for the selection. • This defines what justification is to be provided by the ST author
FMT_SAE.1.2 For each of these security attributes, TSF shall be able to … and *[**ST assignment:** as required by PP, list of ST specific actions to be taken for each ST specific security attribute]* after the expiration time for the indicated security attribute has passed. The ST rationale shall provide a basic justification for the assignment made, to include “null”, showing that it is sufficient to enable secure operation.	• The ST will provide information about the security functions and mechanisms not available to the PP author. • By requiring justification from the ST author, the validity of the completion can be determined.
FMT_SMR.1.1 The TSF shall maintain the roles [**assignment:** … and/or the following set of ST specific roles that the ST author wishes to specify as not conflicting with CSPP goals and useful in implementing these goals: *[**ST assignment:** as allowed by PP, the ST specific authorized identified roles]*]. The ST rationale shall provide a basic justification for the assignment made, showing that the roles specified do not conflict with PP design goals.	• Specifics of the TOE design may result in a preferred choice for the assignment. • At the level of abstraction of the PP any assignment is acceptable provided it is justified in the ST as being consistent with other CSPP requirements.
FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [**assignment:** those indicated in the following ST assignment: *[**ST assignment:** list of TSF failures for which the ST is able to preserve a secure state]*]. As the purpose of this requirement is to make the list of recoverable failures explicit, not to mandate specific failures, the ST rationale does not need to show completeness. However, the ST rationale does need to provide a basic justification for the claim that the ST will preserve a secure state for each failure type listed.	• The specifics of the ST design will likely dictate which failures from which the system can reasonably expect to recover. • It is considered most important to have an explicit list than to specify what the list must contain. The ST must, however, support the claim that recovery is possible.

Functional Operations Deferred to ST	Rationale for Deferring to ST
FPT_RCV.2.2 For [**assignment:** those failures indicated in the following ST assignment: *[**ST assignment:** as required by PP, list of ST specific types of TSF failures]*], the TSF shall ensure the return of the TOE to a secure state using automated procedures. As the purpose here is to ensure that the choice is made explicit, the ST rationale does not need to justify completeness, but does need to provide a basic justification for the claim that the ST will automatically recover from the failure types listed.	• The specifics of the ST design will likely dictate which failures from which the system can reasonably expect to recover. • It is considered most important to have an explicit list than to specify what the list must contain. The ST must, however, support the claim that recovery is possible.
FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [**assignment:** information critical to security in maintaining a consistent state representation across distributed systems as identified in *[**ST assignment:** list of TSF data types]* when shared between the TSF and another trusted IT product. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to provide a broader definition, rather than selecting only a subset - provided the rationale shows that the security critical elements are indeed a subset of those chosen.	• It is anticipated that the specifics of the ST design will play a role in the determination of the specific data elements. • This defines the justification that the ST author must provide. This also provides guidance on what constitutes an acceptable completion.
FPT_TDC.1.2 The TSF shall use [**assignment:** the following interpretation rules: *[**ST assignment:** list of interpretation rules to be applied by the TSF]* when interpreting the TSF data from another trusted IT product. The ST rationale shall provide a basic justification, showing that the list of rules is comprehensive and internally self-consistent.	• It is anticipated that the specifics of the ST design will play a role in the determination of the specific data elements. • This defines the justification that the ST author must provide.
FRU_RSA.1.1-CSPP The TSF shall enforce maximum quotas of the following resources: … that *[**ST selection:** an individual user, a defined group of users, subjects]* can use *[**ST selection:** simultaneously, over a specified period of time]*. The ST rationale must show that the list of resources for which maximum quotas is enforced is sufficiently complete to accomplish protection against resource exhaustion, to the extent that the OS is capable of doing so. Also the ST rationale must give, for both ST selections, the reasoning for the choices made and stating why the choices support the goal of protecting against denial-of-service.	• For both selections, the ST author may select as appropriate, with constraints given in the refinement. • This defines the justification that the ST author must provide.
FTA_LSA.1.1 The TSF shall provide the capability to restrict the scope of these session security attributes: [**assignment:** user role, specific user capabilities, and any *[**ST assignment:** ST specific session security attributes]*], based on [**assignment:** user identity, point of entry, time of day, day of week, and any *[**ST assignment:** attributes specific to the ST design]*]. The ST rationale shall provide a basic justification, showing that the ST specific assignments are sufficient to restrict the security critical attributes.	• The OS must provide the capability to restrict, rather than enforce with without the possibility of user choice to the contrary. • Second refinement ('these') is editorial. • Specifics of the ST design play an important role in determining both the session security attributes and what is used to control these attributes. • The refinement defines the required justification.
FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**assignment:** attributes that can be set by explicitly authorized security administrator(s) or security administrator role(s), including user identity, port of entry, time	

Functional Operations Deferred to ST	Rationale for Deferring to ST
of day, day of the week, and any *[**ST assignment:** ST specific attributes]* . The ST rationale must show that the ST assignment is complete.	• ST design will likely play a role. • This defines the required justification.
FTP_ITC.1.2 The TSF shall permit *[**ST selection:** the TSF, the remote trusted IT product]* to initiate communication via the trusted channel. The ST rationale shall provide a basic justification, showing that the ST selection is appropriate for maintaining secure operation in the intended environment.	• This is deferred because the ST design will play a major role. • This defines the required justification.
FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**assignment:** the following functions: ***[ST assignment:*** *list of functions for which a trusted channel is required]*]. The ST rationale shall provide a basic justification, showing that the ST assignment is a complete list, as required to mitigate insecurities in the intended operational environment for the TOE.	• This is deferred because the ST design will play a major role. • This defines the required justification.
FTP_TRP.1.3 The TSF shall require the use of the trusted path for … [**assignment:** …, and the following: ***[ST assignment:*** *list of additional services for which a trusted path is required, as determined during the ST design and development]*]. The ST rationale shall provide a basic justification, showing that the ST assignments are complete, with regard to mitigation in the intended operational environment for the TOE.	• This is deferred because the ST design will play a major role. • This defines the required justification.

Table 4.3.2-3 Correct Functionality – Rationale for Functional Extensions

Functional Extension	Rationale for the Extension
Extension: FAU_GEN.1-CSPP.3 When the TSF provides application support it shall support an application program interface that allows a privileged application to append data to the security audit trail or to an application-specified alternative security audit trail.	• An API for audit is a reasonable baseline requirement that is not explicitly captured by any CC functional elements.
Extension: FAU_SEL.1-CSPP.2 The TSF shall provide only explicitly authorized user roles, user groups, or individually identified users with the ability to select or display which events are to be audited.	• The 'management' requirement, while deleted from the final version of the CC, is considered appropriate and as a nice 'handle' for the extension below.
FAU_SEL.1-CSPP.3 The TSF shall provide the capability of FAU_SEL.1-CSPP.2 at any time during the operation of the TOE.	• It is considered reasonable to include this non-CC requirement.
Extension: FDP_ACF.1-CSPP.5 The TSF shall provide the capability to assign a user to be a member of more than one user group simultaneously.	• This common capability is of great usefulness but not currently captured within the CC.
FDP_ACF.1-CSPP.6 The TSF shall enforce the rules for authorizing and denying access based upon the CSPP precedence rules.	• This is considered to be a reasonable, baseline requirement, but is not presently in the CC.
Extension: FDP_ETC.1-CSPP.3 The TSF shall shall provide for outgoing information channels, for example TCP port numbers, that are under the control of the TSF and for which general application programs do not have access, when exporting user data controlled under the SFP outside the TSC.	• This is a reasonable requirement that is captured in the CC for incoming information (FDP_ITC) but is missing for outgoing information.
FPT_ITI.1.1-CSPP The TSF shall … the capability to detect modification of [**extension:** security state information that is critical to maintaining a secure state among distributed systems as identified in *[**ST assignment:** list of TSF data requiring such protection]*] data during transmission between TSF and a remote trusted IT product within the following metric: *[**ST assignment**: a defined modification metric or metrics]*. [**extension:** The first ST assignment may be a 'null' list if the ST rationale shows that meeting FPT_ITI.1.2 is sufficient to maintain secure operation.] The ST rationale shall provide a basic justification, showing that the first ST assignment is complete and that the metric, or metrics, called out in the second assignment are sufficient. It is acceptable to protect all data, rather than selecting specific data elements.	• Rather than "all data", it is considered more realistic to narrow the scope. • The ST design will play a role here. • The ST design will play a role here. • It is conceivable that meeting ITI.1.2 will be satisfactory. • This defines the justification required and also provides information on what constitutes an acceptable completion.
FPT_ITI.1.2-CSPP The TSF shall … the capability to verify the integrity of [***extension:*** security state information that is critical to maintaining a secure state among distributed systems as	• Rather than "all data", it is considered more realistic to narrow the scope. • The ST design will play a role here.

Functional Extension	**Rationale for the Extension**
identified in [***ST assignment:*** *list of TSF data requiring such protection]*] transmitted between the TSF and a remote trusted IT product and perform …. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to protect all data, rather than selecting specific data elements.	• This defines the justification required and also provides information on what constitutes an acceptable completion.
FPT_RPL.1.1-CSPP The TSF shall detect replay for the following entities [**extension:** security state information that is critical to maintaining a secure state among distributed systems as identified in [***ST assignment:*** *list of TSF data requiring such protection]*]. The ST rationale shall provide a basic justification, showing that the ST assignment is complete. It is acceptable to protect all communications, rather than selecting specific entities.	• The ST design will play a role here. • This defines the justification required and also provides information on what constitutes an acceptable completion.
Extension: FPT_SYN-CSPP.1.1 The TSF shall support the system capability to provide the capability to synchronize distributed TSF elements and to associate audit event records produced by multiple TSF entities.	• This component is used in lieu of FPT_STM to specify the need instead of a mechanism which could help meet the need. (Refinement is applied to component as stated in [CSPP].)
FTA_MCS.1.1-CSPP The TSF shall [**extension:** enable an authorized user to specify whether or not to] restrict the maximum number of concurrent sessions that belong to the same user.	• Since limiting concurrent sessions is policy specific, it is considered appropriate to make limiting concurrent sessions a parameter.
FTP_ITC.1.1-CSPP The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the [**extension**: security information as required to mitigate against insecurities resulting from both attacks and unintentional modification, to include the following: [***ST assignment:*** *other security information identified in the ST design and development]*] channel data from modification and [**extension**: identification and authentication data and the following other security information: [***ST assignment:*** *other security information identified in the ST design and development*] channel data from disclosure. The ST rationale shall provide a basic justification, showing that the ST assignments are complete, with regard to mitigation in the intended operational environment for the TOE.	• Rather than “all data”, it is considered more realistic to narrow the scope. • The ST design will play a role here. • Rather than “all data”, it is considered more realistic to narrow the scope. • The ST design will play a role here. • This defines the justification required.
FTP_TRP.1.1-CSPP The TSF shall protection of the [**extension**: security information as required to mitigate against insecurities resulting from both attacks and unintentional modification, to include the following: [***ST assignment:*** *other security information identified in the ST design and development]*] communicated data from modification and [**extension**: identification and authentication data and the following other security information: [***ST assignment:*** *other security information identified in the ST design and development*] communicated data from disclosure. The ST	• Rather than “all data”, it is considered more realistic to narrow the scope. • The ST design will play a role here. • Rather than “all data”, it is considered more realistic to narrow the scope. • The ST design will play a role here. • This defines the justification required.

Functional Extension	Rationale for the Extension
rationale shall provide a basic justification, showing that the ST assignments are complete, with regard to mitigation in the intended operational environment for the TOE.	

5.0 ASSURANCE REQUIREMENTS RATIONALE

5.1 NECESSARY ASSURANCES

5.1.1 Basic Assurance Goals

CSPP-OS provides a definition for near-term achievable, low evaluation cost, COTS security. In keeping with this purpose, the assurance components of this protection profile have been selected to (1) require only current best-practice development actions and (2) include minimal third-party analysis. The rationale for each is given below.

The need to constrain requirements for developer actions is clearly evident in order to meet "near-term achievable". The current COTS development standards do not include security engineering to any significant degree. Adding such techniques and processes would require changes to development practices and personnel capabilities. Since such changes are not considered likely, CSPP-OS has been developed with that in mind.

The rationale for limiting third-party analysis is:

a. Technical basis. In keeping with current best commercial practice, CSPP-OS requirements do not include significant security engineering. Therefore, there is no reasonable expectation of high security quality with respect to effectiveness in the face of competent threat agents. Moreover, the most likely internal structures for CSPP-OS components make comprehensive evaluation extremely difficult, if not, for all practical purposes, impossible. Hence, the probability of exploitable vulnerabilities in CSPP-OS compliant components is not significantly different than that of non-compliant COTS. Since there is no reasonable expectation for high security quality in CSPP-OS components (even with an extensive evaluation), there is no technical basis for extensive evaluation of CSPP-OS class components.

b. Business-case basis. In order to support a good business case, CSPP-OS evaluation must be achievable without negative impact on customer acceptance over non-evaluated competition. Since CSPP-OS vendors cannot reasonably claim high security quality, CSPP-OS evaluation is unlikely to be a discriminator overcoming cost and time-to-market. Hence, the CSPP-OS evaluation provides a market advantage if evaluated products are competitive against non-evaluated products on the basis of cost and time-to-market. Therefore, a CSPP-OS evaluation must be low cost and of short duration.

5.1.2 EAL Selection

This section provides a rationale for the selection of EAL2 as the base EAL for EAL-CSPP. This will be accomplished by first describing why EAL1 is not sufficient and then describing why EAL3 is too much for the basic goals for CSPP-OS. Since the EALs are strictly hierarchical, the rationale for not selecting EAL4 through EAL7 is covered by that given for EAL3.

a. EAL1 not sufficient. Table 5.1.2-1 lists the assurance components contained in EAL2 which are not a part of EAL1, describing why they are required assurances for CSPP-OS. Since EAL1 lacks these components, it is not sufficient as the base EAL.

Table 5.1.2-1 Necessary Assurance - EAL1 Not Sufficient

EAL2 Component not in EAL1	Component Title	Why Required in CSPP-OS
ACM_CAP.2 (EAL-1 has CAP.1)	Configuration items	It is well within best commercial practice for a security product vendor to have CM documentation and to be able to uniquely identify all configuration items. Since it is reasonable to expect this, the assurance it offers should be a part of CSPP-OS.
ADO_DEL.1	Delivery procedures	This component requires that the vendor have procedures for “secure” delivery to the customer. Since (1) software piracy controls will be implemented and (2) the CSPP-OS requirement does not specify a specific set of procedures, this component is within the range of best commercial practice and should be a part of CSPP-OS.
ADO_IGS.1	Installation, generation, and start-up procedures	It is necessary and reasonable to expect an IT security product to include guidance to the user on secure installation, generation, and start-up. Therefore this must be a part of an effective CSPP-OS.
ADV_HDL.1	Descriptive high-level design	If using best commercial practice, the vendor can be expected to have the high-level design for the TOE required by this component. Since it is a reasonable expectation, it should be included in CSPP-OS.
ATE_IND.2 (EAL1 has IND.1)	Independent testing – sample	Having the evaluator execute a sample of the vendor tests, as a check on their validity, is a low-cost, reasonable action well within the bounds of the basic goals for CSPP-OS assurance.
AVA_SOF.1	Strength of TOE security function evaluation	This is a vendor driven requirement, in that the only analysis required is for security functionality for which the security target includes a claim of strength of function. If the claim is not made, no analysis is required. If the claim is made, then requiring an analysis is a reasonable expectation and should be a part of CSPP-OS.

EAL2 Component not in EAL1	Component Title	Why Required in CSPP-OS
AVA_VLA.1	Developer vulnerability analysis	It is an essential part of the CSPP-OS basic assurance level that at least obvious; and common, public-domain; vulnerabilities are addressed.

b. EAL3 too much. Table 5.1.2-2 lists the assurance components contained in EAL3 which are not a part of EAL2, describing those that are not appropriate for CSPP-OS. Since EAL3 contains these components, it is too much for the base EAL. Because of the hierarchical nature of the EALs, EAL4 through EAL7 are also too much, leaving EAL2 as the best choice.

Table 5.1.2-2 Necessary Assurance - EAL3 Too Much

EAL3 Component Not in EAL2	Component Title	Why not appropriate for CSPP-OS
ACM_CAP.3 (EAL2 has CAP.2)	Authorization controls	N/A – included in EAL-CSPP
ACM_SCP.1	TOE CM coverage	N/A – included in EAL-CSPP as part of the CSPP-OS requirement for ACM_SCP.2
ADV_HLD.2	Security enforcing high-level design	This component is the reason EAL3 is not acceptable as the base level for CSPP-OS. The requirement to “describe the separation of the TSF into TSP enforcing and other subsystems” reflects a degree of and capability for security engineering that is not a part of current (or expected near-term) standard COTS development. Although most of EAL3 is a part of EAL-CSPP, the CC explicitly forbids calling out an EAL subset. Therefore, not wanting this component of EAL3 necessitates going to an augmented version of the next lower EAL (EAL2).
ALC_DVS.1	Identification of security measures	N/A – included in EAL-CSPP
ATE_COV.2 (EAL2 has COV.1)	Analysis of coverage	N/A – included in EAL-CSPP
ATE_DPT.1	Testing: high level design	N/A – included in EAL-CSPP
AVA_MSU.1	Examination of guidance	N/A – included in EAL-CSPP as part of the CSPP-OS requirement for AVA_MSU.3

5.1.3 EAL Augmentation

Table 5.1.3-1 gives the rationale for each CC assurance component in EAL-CSPP that is an augmentation to the base EAL2 level.

Table 5.1.3-1 Necessary Assurance - Augmentation Rationale

Component	Component Title	Rationale for Augmentation
ACM_CAP.3	Authorization controls	Note: EAL2 includes ACM_CAP.2. ACM_CAP.3 adds the requirement for a CM plan and its use. A quality IT vendor developing secure products can be reasonably expected to provide this CM. The use of a CM plan is within the bounds of standard, best commercial practice for IT development.
ACM_SCP.2	Problem tracking CM coverage	Note: EAL2 has no ACM_SCP component. A CSPP-OS vendor can be expected to apply CM to the items called out in ACM_SCP.2. Specifically, since the product is security related, the tracking of security flaws is a very reasonable expectation and within the bounds of standard, best commercial practice.
ADV_SPM.1	Informal TOE security policy model	This assurance component is a required dependency for the following, essential functional requirements: FMT_MSA.3 Static attribute initialization FPT_FLS.1 Failure with preservation of secure state FPT_RCV.2 Automated Recovery While the generation of a security policy does require security expertise, this can be performed by a consultant (if necessary) and does not otherwise impact the vendor's existing development process.
ALC_DVS.1	Identification of security measures	This component requires the definition and implementation of protective security measures during IT development. Since there is no requirement for a specific set of measures, the vendor is largely free to state his procedures as they exist. Therefore, this imposes no undue burden on the vendor and is within the scope of standard, best commercial practice.

Component	Component Title	Rationale for Augmentation
ALC_FLR.2	Flaw reporting procedures	Note: EAL2 has no ALC_FLR component. It is well within standard, best commercial practice for a vendor of security products to have flaw remediation procedures covering acting upon user reports, correcting flaws, notifying users, and reducing the potential for introducing new flaws. Specific procedures are not indicated in the assurance requirement, therefore there is minimal impact on any vendor who is already accomplishing the intent of the requirement.
ATE_COV.2	Analysis of coverage	Note: EAL2 has ALC_COV.1. It is reasonable to require a security vendor implementing best commercial practice to demonstrate that the vendor testing completely covers the security functionality called out in the vendor produced functional specification.
ATE_DPT.1	Testing: high level design	This component requires that the vendor analyze the vendor testing to demonstrate that it verifies the high-level design. For a competent, security vendor implementing best commercial practices, this should be of little impact to existing development activities.
AVA_MSU.2	Validation of analysis	Note: EAL2 has no AVA_MSU component. A security vendor implementing standard, best commercial practices will not be impacted by this component. AVA_MSU.2 requires that the vendor produce user and administrator documentation that is adequate for understanding the operating modes of the TOE and the required external security controls necessary for secure operation. The vendor is required to analyze this documentation for conformance to the requirements. The other AVA_MSU.2 requirements fall onto the evaluator. AVA_MSU.2 is essential in covering T.OBSERVE and is important in covering P.SURVIVE T.CRASH T.INSTALL T.OPERATE

5.2 SUFFICIENT ASSURANCES

Table 5.2-1 maps unused CC assurance components to the rationale for non-selection.

Table 5.2-1 Complete Assurance - Non-Selection Rationale

Component	Component Title	Why Not Included in EAL-CSPP
Family ACM_AUT	CM Automation	While automation of the CM process can be beneficial, it is simply not a key factor in determining the security quality for CSPP-OS compliant TOEs. A vendor can use the fact that his CM includes automated processes as justification for meeting other requirements, but automation is not, itself, a requirement.
ACM_CAP.4 ACM_CAP.5	Generation support and acceptance procedures Advanced support	While the vendor may have CM procedures covering TOE generation (CAP.4) and integration (CAP.5), these are much less likely to be a part of the existing vendor practices than those included with the EAL-CSPP requirement for ACM_CAP.3.
ACM_SCP.3	Development tools CM coverage	Full CM coverage of developmental tools is not a part of standard, best commercial practice and is therefore beyond the scope of the basic goals for CSPP-OS assurance.
ADO_DEL.2 ADO_DEL.3	Detection of modification Prevention of modification	ADO_DEL.2 and DEL.3 are not part of standard, best commercial practice and therefore are beyond the scope of the basic goals for CSPP-OS assurance.
ADO_IGS.2	Generation log	The requirement for a generation log is not a part of standard, best commercial practice and is therefore beyond the scope of the basic goals for CSPP-OS assurance.
ADV_FSP.2 ADV_FSP.3 ADV_FSP.4	Fully defined external interfaces Semiformal functional specification Formal functional specification	While good ideas, fully defined interfaces and semiformal or formal specification are not at part of existing best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP-OS assurance.
ADV_HLD.2 ADV_HLD.3 ADV_HLD.4 ADV_HLD.5	Security enforcing high-level design Semiformal high-level design Semiformal high-level explanation Formal high-level design	The requirements of ADV_HLD.2 include security engineering that is not a part of existing best commercial practices. This is sufficient to make all of these components beyond the scope of the basic goals for CSPP-OS assurance.

Component	Component Title	Why Not Included in EAL-CSPP
Family ADV_IMP	Implementation representation	It is not reasonable, either from the CSPP-OS goal to limit evaluation cost and time or the CSPP-OS goal to keep within the bounds of best commercial practice to include implementation representation requirements.
Family ADV_INT	TSF internals	It is clearly outside the bounds of current best commercial practice to include these requirements on TSF internals. To require these would necessitate major changes to the vendor's development practices. Such changes are beyond the scope of the basic goals for CSPP-OS assurance.
Family ADV_LLD	Low-level design	It is not reasonable, either from the CSPP-OS goal to limit evaluation cost and time or the CSPP-OS goal to keep within the bounds of best commercial practice to include low-level design requirements.
ADV_RCR.2 ADV_RCR.3	Semiformal correspondence demonstration Formal correspondence demonstration	Semiformal or formal requirements are not a part of existing, best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP-OS assurance.
ADV_SMP.2 ADV_SMP.3	Semiformal TOE security policy model Formal TOE security policy model	Semiformal or formal requirements are not a part of existing, best commercial practice. Therefore these are beyond the scope of the basic goals for CSPP-OS assurance.
ALC_DVS.2	Sufficiency of security measures	This requirement may necessitate major changes to existing, vendor development practices, even where standard, best commercial practices are being implemented. Therefore these are beyond the scope of the basic goals for CSPP-OS assurance.
ALC_FLR.3	Systematic flaw remediation	It is beyond best commercial practices to require specific points of contact for flaw reporting and the automatic distribution of flaw reports. Therefore this component is beyond the scope of the basic goals for CSPP-OS assurance.
Family ALC_LCD	Life cycle definition	Current best commercial practices do not include clearly defined life-cycle models. While this may become standard, it is not at present. Therefore this family is beyond the scope of the basic goals for CSPP-OS assurance.

Component	Component Title	Why Not Included in EAL-CSPP
Family ALC_TAT	Tools and techniques	Current best commercial practices do not include these requirements on the definition and control of all tools used in the development. Moreover, this family has ADV_IMP as a required dependency and, as already explained, ADV_IMP is beyond the scope of the basic goals for CSPP-OS assurance.
ATE_COV.3	Rigorous analysis of coverage	It is well outside the bounds of current, best commercial practices to require a rigorous analysis of vendor testing. Therefore this component is beyond the scope of the basic goals for CSPP-OS assurance.
ATE_DPT.2 ATE_DPT.3	Testing – low level design Testing – implementation representation	Since the low-level design and implementation requirements are beyond scope and not included in CSPP-OS, these depth of testing requirements are also beyond the scope of the basic goals for CSPP-OS assurance.
ATE_FUN.2	Ordered functional testing	The requirement for analysis of test ordering dependencies is not part of best commercial practices and hence is beyond the scope of the basic goals for CSPP-OS assurance.
ATE_IND.3	Independent testing – complete	This requirement adds unnecessary time and cost to the evaluation. Therefore it is beyond the scope of the basic goals for CSPP-OS assurance.
Family AVA_CCA	Covert channel analysis	Covert channel analysis is not a part of existing best commercial practice and therefore is beyond the scope of the basic goals for CSPP-OS assurance.
AVA_MSU.3	Analysis and testing for insecure states	While this component might be considered within the range of best commercial practices, it is outside the scope of near-term, mutual recognition agreements and hence has not been selected for CSPP-OS.
AVA_VLA.2 AVA_VLA.3 AVA_VLA.4	Independent vulnerability analysis Moderately resistant Highly resistant	The requirements already a part of CSPP-OS through AVA_VLA.1 include evaluator penetration testing, and additional evaluator actions would be beyond the scope of the basic goals for CSPP-OS assurance. Moreover, the reasonable expectations for CSPP-OS compliant TOEs do not include the potential for resistance to penetration.
AMA_AMP	Assurance maintenance plan	This family is beyond the scope of the basic goals for CSPP-OS assurance.

Component	Component Title	Why Not Included in EAL-CSPP
AMA_CAT	TOE component categorization report	While a case can be made for inclusion of this family as part of CSPP-OS, AMA_CAT is not covered by near-term, mutual recognition agreements and is therefore excluded from CSPP-OS.
AMA_EVD	Evidence of assurance maintenance	This family does not apply to an initial evaluation.
AMA_SIA	Security impact analysis	This family does not apply to an initial evaluation.

5.3 CORRECT ASSURANCES

5.3.1 Dependencies for assurances

Table 5.3.1-1 shows correctness of the assurances with respect to meeting all dependencies.

Table 5.3.1-1 Correct Assurances – Dependency Mapping

Item #	Component	Component Title	Dependency	Item #
1	ACM_CAP.3	Authorization controls	ACM_SCP.1 ALC_DVS.1	2* 11
2	ACM_SCP.2	Problem tracking CM Coverage	ACM_CAP.3	1
3	ADO_DEL.1	Delivery procedures	—	—
4	ADO_IGS.1	Installation, Generation, and Start-up Procedures	AGD_ADM.1	9
5	ADV_FSP.1	Informal functional specification	ADV_RCR.1	7
6	ADV_HLD.1	Descriptive High-Level Design	ADV_FSP.1 ADV_RCR.1	5 7
7	ADV_RCR.1	Informal Correspondence Demonstration	—	—
8	ADV_SPM.1	Informal TOE security policy model	ADV_FSP.1	5
9	AGD_ADM.1	Administrator Guidance	ADV_FSP.1	5
10	AGD_USR.1	User Guidance	ADV_FSP.1	5
11	ALC_DVS.1	Identification of Security Measures	—	—
12	ALC_FLR.2	Flaw reporting procedures	—	—
13	ATE_COV.2	Analysis of coverage	ADV_FSP.1 ATE_FUN.1	5 15
14	ATE_DPT.1	Testing: High-Level Design	ADV_HLD.1 ATE_FUN.1	6 15
15	ATE_FUN.1	Functional Testing	—	—
16	ATE_IND.2	Independent Testing - Sample	ADV_FSP.1 AGD_ADM.1 AGD_USR.1 ATE_FUN.1	5 9 10 15
17	AVA_MSU.2	Validation of analysis	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	4 5 9 10
18	AVA_SOF.1	Strength of TOE Security Function Evaluation	ADV_FSP.1 ADV_HLD.1	5 6

Item #	Component	Component Title	Dependency	Item #
19	AVA_VLA.1	Developer vulnerability Analysis	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	5 6 9 10

* - indicates that this dependency is covered by a strictly hierarchical component

5.3.2 Assurance Operations

There are no operations performed on assurance components in CSPP-OS.

6.0 APPENDIX A - REFERENCES

[CSPP] *CSPP - Guidance for COTS Security Protection Profiles*, version 1.0, December 1999.

[CSPP-OS] CSPP-OS - COTS Security Protection Profile - Operating Systems, Draft, version 0.3, 12/9/99

[CC-V2] *Common Criteria for Information Technology Security Evaluation*, May 1998.